Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other material provided with the distribution.

Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided by the copyright holders and contributors “as is” and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright holder or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

This software is provided by Cambridge Broadband Ltd “as is” and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright holder be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. For a copy of the GNU Lesser General Public License, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details. For a copy of the GNU Library General Public License, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.
## Table of Contents

### About This Guide

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before You Begin</td>
<td>ix</td>
</tr>
<tr>
<td>Audience</td>
<td>ix</td>
</tr>
<tr>
<td>What’s In This Manual</td>
<td>ix</td>
</tr>
<tr>
<td>Typographical Conventions</td>
<td>ix</td>
</tr>
<tr>
<td>Editions/Used In</td>
<td>xi</td>
</tr>
<tr>
<td>Syntax</td>
<td>xii</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>xii</td>
</tr>
<tr>
<td>Steel-Belted Radius Documentation</td>
<td>xii</td>
</tr>
<tr>
<td>Requests for Comments (RFCs)</td>
<td>xiii</td>
</tr>
<tr>
<td>Third-Party Products</td>
<td>xiv</td>
</tr>
<tr>
<td>Contacting Technical Support</td>
<td>xiv</td>
</tr>
</tbody>
</table>

### Chapter 1  Introduction

Configuration Files ................................................................. 1

### Chapter 2  Operations Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>access.ini File</td>
<td>8</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>8</td>
</tr>
<tr>
<td>[Users] and [Groups] Sections</td>
<td>8</td>
</tr>
<tr>
<td>admin.ini File</td>
<td>10</td>
</tr>
<tr>
<td>[AccessLevel] Section</td>
<td>10</td>
</tr>
<tr>
<td>[SNMPAgent] Section (GEE/SPE only)</td>
<td>13</td>
</tr>
<tr>
<td>bounce.ini File (Windows only)</td>
<td>15</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>15</td>
</tr>
<tr>
<td>ccagw.ini File</td>
<td>17</td>
</tr>
<tr>
<td>[gateway] section</td>
<td>17</td>
</tr>
<tr>
<td>eval.ini File</td>
<td>18</td>
</tr>
<tr>
<td>events.ini File</td>
<td>19</td>
</tr>
<tr>
<td>[EventDilutions] Section</td>
<td>19</td>
</tr>
<tr>
<td>[Suppress] Section</td>
<td>19</td>
</tr>
<tr>
<td>[Thresholds] Section</td>
<td>20</td>
</tr>
<tr>
<td>radius.ini File</td>
<td>22</td>
</tr>
<tr>
<td>[Addresses] Section</td>
<td>22</td>
</tr>
<tr>
<td>[AuditLog] Section</td>
<td>23</td>
</tr>
<tr>
<td>[AuthRejectLog] Section</td>
<td>24</td>
</tr>
<tr>
<td>[Configuration] Section</td>
<td>26</td>
</tr>
<tr>
<td>[CurrentSessions] Section</td>
<td>35</td>
</tr>
<tr>
<td>[Debug] Section</td>
<td>35</td>
</tr>
<tr>
<td>[EmbedInClass] Section</td>
<td>36</td>
</tr>
<tr>
<td>[FailedAuthOriginStats] Section (Windows only)</td>
<td>36</td>
</tr>
<tr>
<td>[HiddenEAPIdentity] Section</td>
<td>37</td>
</tr>
<tr>
<td>[IPPoolSuffixes] Section</td>
<td>38</td>
</tr>
</tbody>
</table>
### Table of Contents

#### Chapter 3  Authentication Configuration Files

<table>
<thead>
<tr>
<th>File</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[IPv6] Section</td>
<td>38</td>
</tr>
<tr>
<td>[LDAP] Section</td>
<td>39</td>
</tr>
<tr>
<td>[LDAPAddresses] Section</td>
<td>40</td>
</tr>
<tr>
<td>[MsChapNameStripping] Section</td>
<td>40</td>
</tr>
<tr>
<td>[Ports] Section</td>
<td>42</td>
</tr>
<tr>
<td>[SecurID] Section</td>
<td>44</td>
</tr>
<tr>
<td>[Self] Section</td>
<td>44</td>
</tr>
<tr>
<td>[StaticAcctProxy] Section</td>
<td>45</td>
</tr>
<tr>
<td>[Strip] Section</td>
<td>45</td>
</tr>
<tr>
<td>[StripPrefix] Section</td>
<td>46</td>
</tr>
<tr>
<td>[StripSuffix] Section</td>
<td>46</td>
</tr>
<tr>
<td>[UserNameTransform] Section</td>
<td>46</td>
</tr>
<tr>
<td>[ValidateAuth] and [ValidateAcct] Sections</td>
<td>48</td>
</tr>
<tr>
<td>sbrd.conf File (Solaris/Linux only)</td>
<td>50</td>
</tr>
<tr>
<td>services File</td>
<td>53</td>
</tr>
<tr>
<td>servtype.ini File</td>
<td>55</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>55</td>
</tr>
<tr>
<td>[NAS] Section</td>
<td>56</td>
</tr>
<tr>
<td>[MappingName] Section</td>
<td>56</td>
</tr>
<tr>
<td>Example</td>
<td>56</td>
</tr>
<tr>
<td>update.ini File</td>
<td>58</td>
</tr>
<tr>
<td>[HUP] and [USR2] Sections</td>
<td>58</td>
</tr>
<tr>
<td>Auto-Restart Files (Solaris/Linux only)</td>
<td>62</td>
</tr>
<tr>
<td>Perl SNMP Support</td>
<td>62</td>
</tr>
<tr>
<td>Perl syslog Support</td>
<td>62</td>
</tr>
<tr>
<td>S90radius/sbrd Script</td>
<td>62</td>
</tr>
<tr>
<td>radiusd Script</td>
<td>63</td>
</tr>
<tr>
<td>authlog.ini File</td>
<td>68</td>
</tr>
<tr>
<td>[Alias/name] Sections</td>
<td>68</td>
</tr>
<tr>
<td>[Attributes] Section</td>
<td>69</td>
</tr>
<tr>
<td>[Configuration] Section</td>
<td>69</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>70</td>
</tr>
<tr>
<td>authReport.ini File</td>
<td>73</td>
</tr>
<tr>
<td>[AcceptReport] Section</td>
<td>73</td>
</tr>
<tr>
<td>[BadSharedSecretReport] Section</td>
<td>73</td>
</tr>
<tr>
<td>[RejectReport] Section</td>
<td>74</td>
</tr>
<tr>
<td>[UnknownClientReport] Section</td>
<td>74</td>
</tr>
<tr>
<td>authReportAccept.ini File</td>
<td>75</td>
</tr>
<tr>
<td>[Attributes] Section</td>
<td>75</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>75</td>
</tr>
<tr>
<td>authReportBadSharedSecret.ini File</td>
<td>78</td>
</tr>
<tr>
<td>[Attributes] Section</td>
<td>78</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>79</td>
</tr>
<tr>
<td>authReportReject.ini File</td>
<td>81</td>
</tr>
<tr>
<td>[Attributes] Section</td>
<td>81</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>82</td>
</tr>
<tr>
<td>authReportUnknownClient.ini File</td>
<td>85</td>
</tr>
<tr>
<td>[Attributes] Section</td>
<td>85</td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>86</td>
</tr>
<tr>
<td>blacklist.ini File</td>
<td>88</td>
</tr>
<tr>
<td>lockout.ini File</td>
<td>89</td>
</tr>
<tr>
<td>redirect.ini File</td>
<td>90</td>
</tr>
</tbody>
</table>
Chapter 4  **Attribute Processing Files**

Overview .......................................................... 109
  Dictionary File Location ........................................... 110
  Dictionary File Records ........................................ 110
  Editing Dictionary Files ........................................ 111
  Include Records .................................................. 111
  ATTRIBUTE Records ........................................... 112
  Macro Records .................................................... 115
  OPTION Records ................................................ 116
  classmap.ini File .................................................. 117
    [AttributeName] Section ...................................... 117
  filter.ini File ....................................................... 119
    Filter Rules ..................................................... 119
    Order of Filter Rules .......................................... 120
    Values in Filter Rules ........................................ 121
    Referencing Attribute Filters ................................ 122
  sample.rr File ...................................................... 124
  spi.ini File .......................................................... 126
    [Keys] Section .................................................. 126
    [Hosts] Section ................................................ 127
  vendor.ini File ..................................................... 128
    [Vendor-Product Identification] Section .................. 128
      Product-Scan Settings .................................... 130

Chapter 5  **Address Assignment Files**

dhcp.ini File ......................................................... 134
  [Settings] Section ............................................... 134
  [Pools] Section .................................................... 135
  pool.dhc Files ..................................................... 136
    [Settings] Section ............................................... 136
    [Request] Section .............................................. 136
    [Reply] Section ................................................ 138
    Reconfiguring Pools .......................................... 138

Chapter 6  **Accounting Configuration Files**

account.ini File ..................................................... 142
  [Alias/name] Sections .......................................... 142
  [Attributes] Section .......................................... 143
Chapter 7  Realm Configuration Files  149

Proxy Realm Configuration Files  150
Sample radius.ini Realm Settings  150
Examples...  150
Sample Proxy RADIUS (.pro) File  151
Sample filter.ini File  152
Directed Realm Configuration Files  153
Sample radius.ini Realm Settings  153
Sample proxy.ini File  153
Sample Directed Realm (.dir) File  154
proxy.ini File  155
[Configuration] Section  155
[Realms] Section...  156
[Directed] Section  156
[Processing] Section  157
[AttributeMap] Sections  157
[DirectedAcctMethods] Section  160
[StaticAcct] Section  160
[Interfaces] Section  162
Proxyrl.ini File  163
Proxy RADIUS Configuration (.pro) File  164
[Auth] Section  164
[Acct] Section  166
[AutoStop] Section  168
[Called-Station-ID] Section  169
Target Selection Rules  170
[FastFail] Section  172
[ModifyUser] Section  173
[SpooledAccounting] Section  174
Directed Realm Configuration (.dir) File  176
[Auth] Section  177
[AuthMethods] Section  177
[Acct] Section  178
[AcctMethods] Section  179
[Called-Station-ID] Section  180
[ModifyUser] Section  180
radius.ini Realm Settings  181

Chapter 8  EAP Configuration Files  183

eap.ini File  184
fastauth.aut File  187
[Bootstrap] Section  187
[Server_Settings] Section  188
[FAST_Protocol] Section  189
[Inner_Authentication] Section  189
[Request Filters] Section  190
[Response Filters] Section  190
Example  191
peapauth.aut File  193
<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>SNMP Configuration Files</th>
<th>223</th>
</tr>
</thead>
<tbody>
<tr>
<td>jnprsnmpd.conf</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>Access Control Section</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>Security Names Section</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>Access View Section</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>Group Access Section</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>System Contact Section</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>Traps Section</td>
<td>226</td>
<td></td>
</tr>
<tr>
<td>SNMP Proxy Section</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>[snmp] Section</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>[snmpd] Section</td>
<td>228</td>
<td></td>
</tr>
<tr>
<td>Subagent Section</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>radiusdir Section</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>testagent.sh</td>
<td>230</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10</th>
<th>SQL Authentication Files</th>
<th>231</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Authentication Header Files</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>[Bootstrap] Section</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>[FailedSuccessResultAttributes] Section</td>
<td>232</td>
<td></td>
</tr>
<tr>
<td>[Failure] Section</td>
<td>233</td>
<td></td>
</tr>
<tr>
<td>[Results] Section</td>
<td>234</td>
<td></td>
</tr>
<tr>
<td>[Server] Section</td>
<td>236</td>
<td></td>
</tr>
<tr>
<td>[Server/name] Sections</td>
<td>237</td>
<td></td>
</tr>
<tr>
<td>[Settings] Section</td>
<td>238</td>
<td></td>
</tr>
<tr>
<td>[Strip] Sections</td>
<td>241</td>
<td></td>
</tr>
</tbody>
</table>
About This Guide

The Steel-Belted Radius Reference Guide describes the configuration options for the Steel-Belted Radius software.

Before You Begin

This manual assumes that you have installed the Steel-Belted Radius software and the SBR Administrator. For more information, refer to the Steel-Belted Radius Getting Started manual.

Audience

This manual is intended for network administrators responsible for implementing and maintaining authentication, authorization, and accounting services for an enterprise. This manual assumes that you are familiar with general RADIUS and networking concepts and the specific environment in which you are installing Steel-Belted Radius.

If you use Steel-Belted Radius with third-party products such as Oracle or RSA SecurID, you should be familiar with their installation, configuration, and use.

What’s In This Manual

This manual contains the following chapters and appendixes:

- Chapter 1, “Introduction,” presents a summary of the files used by the various editions of Steel-Belted Radius and provides some general suggestions about modifying configuration files.
- Chapter 2, “Operations Files,” describes the files used to specify Steel-Belted Radius operation and administration settings.
- Chapter 3, “Authentication Configuration Files,” describes the files used to specify Steel-Belted Radius authentication configuration settings.
- Chapter 4, “Attribute Processing Files,” describes the configuration and dictionary files that specify RADIUS attributes for third-party network devices.
Chapter 5, “Address Assignment Files,” describes the files used to configure address assignment functions in the GEE and SPE versions of Steel-Belted Radius.

Chapter 6, “Accounting Configuration Files,” describes the files used to enable and configure Steel-Belted Radius accounting settings.

Chapter 7, “Realm Configuration Files,” describes the configuration files relating to proxy and directed realm administration in the GEE and SPE versions of Steel-Belted Radius.

Chapter 8, “EAP Configuration Files,” describes the EAP configuration and helper files, which specify options for automatic EAP helper methods.

Chapter 9, “SNMP Configuration Files,” describes the SNMP configuration files used in the GEE and SPE versions of Steel-Belted Radius (Solaris/Linux only).

Chapter 10, “SQL Authentication Files,” describes the files used to configure SQL authentication in Steel-Belted Radius.

Chapter 11, “SQL Accounting Files,” describes the files used configure SQL accounting in Steel-Belted Radius.

Chapter 12, “LDAP Authentication Files,” describes the files used to configure LDAP authentication in Steel-Belted Radius.


Appendix D, “Windows Events,” describes the Windows events that can be generated by Steel-Belted Radius.

### Typographical Conventions

Table 1 describes the text conventions used throughout this manual.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold typeface</td>
<td>Indicates buttons, field names, dialog names, and other user interface elements.</td>
<td>Use the Scheduling and Appointment tabs to schedule a meeting.</td>
</tr>
</tbody>
</table>
Table 1: Typographical Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plain sans serif typeface</strong></td>
<td>Represents:</td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>▪ Code, commands, and keywords</td>
<td>▪ Code:</td>
</tr>
<tr>
<td></td>
<td>▪ URLs, file names, and directories</td>
<td>certAttr.OU = 'Retail Products Group'</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>Identifies:</td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td>▪ Terms defined in text</td>
<td>▪ Defined term:</td>
</tr>
<tr>
<td></td>
<td>▪ Variable elements</td>
<td>An RDP client is a Windows component that enables a</td>
</tr>
<tr>
<td></td>
<td>▪ Book names</td>
<td>connection between a Windows server and a user’s</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machine.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Variable element:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use settings in the Users &gt; Roles &gt; Select Role &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Terminal Services page to create a terminal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>emulation session.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Book name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See the Steel-Belted Radius Administration Guide.</td>
</tr>
</tbody>
</table>

**Editions/Used In**

Steel-Belted Radius is available in multiple editions to meet the requirements of different types of customers. This manual uses the following abbreviations to identify editions of Steel-Belted Radius:

- **GEE** – Global Enterprise Edition
- **SPE** – Service Provider Edition
- **SPE + EAP** – Service Provider Edition with optional EAP Extension Module
- **SPE + MIM** – Service Provider Edition with optional Mobile IP Module
- **EE** – Enterprise Edition

The description of each configuration file used in Steel-Belted Radius identifies the editions that use that file. If an edition uses only some of the settings in a file, the edition identifier includes an asterisk. For example, the following label indicates that the GEE and SPE + EAP editions use all settings in the file, the SPE and SPE + MIM editions use some of the settings in the file, and the EE edition does not use the file.

**Used by:** GEE, SPE*, SPE + MIM*, SPE + EAP  
**Not used by:** EE
Syntax

- `radiusdir` represents the directory into which Steel-Belted Radius has been installed. By default, this is `C:\radius` for Windows systems and `/opt/juniper/radius` on Linux and Solaris systems.

- Brackets `[ ]` enclose optional items in format and syntax descriptions. In the following example, the first `Attribute` argument is required; you can include an optional second `Attribute` argument by entering a comma and the second argument (but not the square brackets) on the same line.

  `<add | replace> = Attribute [, Attribute]`

In configuration files, brackets identify section headers:

```
the [Processing] section of proxy.ini
```

In screen prompts, brackets indicate the default value. For example, if you press Enter without entering anything at the following prompt, the system uses the indicated default value (`/opt`).

```
Enter install path [/opt]:
```

- Angle brackets `< >` enclose a list from which you must choose an item in format and syntax descriptions.

- A vertical bar (`|`) separates items in a list of choices. In the following example, you must specify `add` or `replace` (but not both):

  `<add | replace> = Attribute [, Attribute]`

Related Documentation

The following documents supplement the information in this manual.

Steel-Belted Radius Documentation

Please review the `ReleaseNotes.txt` file that accompanies your Steel-Belted Radius software. This file contains the latest information about features, changes, known problems, and resolved problems. If the information the `ReleaseNotes.txt` file differs from the information found in the Steel-Belted Radius manuals, use the information in the `ReleaseNotes.txt` file.

In addition to this manual, the Steel-Belted Radius documentation includes the following manuals:

- The Steel-Belted Radius Getting Started manual describes how to install the Steel-Belted Radius software on a server running the Solaris operating system, the Linux operating system, or the Windows 2000/Windows XP/Windows Server 2003 operating system.
- The Steel-Belted Radius Administration Guide describes how to configure and administer the Steel-Belted Radius software.

- (SPE Only) The Mobile IP Module Guide describes how the Mobile IP module works and how to configure Steel-Belted Radius/Service Provider Edition to support 3GPP2 or 3GPP services in the Mobile IP module.

Requests for Comments (RFCs)

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFC)s online at http://www.ietf.org/rfc.html. Table 2 lists the RFCs that apply to this guide.

Table 2: RFCs

<table>
<thead>
<tr>
<th>RFC Number</th>
<th>Title</th>
</tr>
</thead>
</table>
Third-Party Products

For more information about configuring your access servers and firewalls, consult the manufacturer’s documentation provided with each device.

Contacting Technical Support

For technical support, contact Juniper Networks at support@juniper.net, or at 1-888-314-JTAC (in the United States) or 408-745-9500 (outside the United States).

Refer to our website (http://www.juniper.net) for additional information and technical notes. When you are running SBR Administrator, you can choose Web > Steel-Belted Radius User Page to access a special home page for Steel-Belted Radius users.

When you call technical support, please have the following information at hand:

- Your Steel-Belted Radius product edition and release number (for example, Global Enterprise Edition version 6.0).
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- Question or description of the problem, with as much detail as possible.
- Any documentation that can help to resolve the problem, such as error messages, memory dumps, compiler listings, and error logs.
Chapter 1
Introduction

Steel-Belted Radius is a complete implementation of the RADIUS (Remote Authentication Dial In User Service) protocol that runs in your Windows, Solaris, or Linux environment. It interfaces with a wide variety of network access devices, and authenticates remote and WLAN users against numerous back-end databases — allowing you to consolidate the administration of all your remote and WLAN users, however they connect to your network.

Configuration Files

The configuration and behavior of your Steel-Belted Radius server is determined by a set of configuration files. In many cases, you must edit these files manually. In a few cases, the contents of a configuration file are updated dynamically when you use the SBR Administrator application to change settings.

Configuration files reside in the \radiusdir\Service (Windows) or radiusdir (Solaris/Linux) directory. The number and names of configuration files depend on which edition of Steel-Belted Radius you are running and whether you are using optional add-on components.

Table 3 identifies the files that are used by each edition of Steel-Belted Radius. An asterisk in an entry means that the applicable edition uses some but not all of the settings in that file.

<table>
<thead>
<tr>
<th>File</th>
<th>Function</th>
<th>GEE</th>
<th>SPE</th>
<th>EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.acc</td>
<td>Configures an SQL accounting method.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>*.dcm</td>
<td>Master list of dictionary files.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>*.dct</td>
<td>Vendor-specific dictionary file.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>*.dhc</td>
<td>Configures specific DHCP address pools, where * is the name of an address pool listed in dhcp.ini.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>*.dir</td>
<td>Configures directed authentication and directed accounting realms.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>File</td>
<td>Function</td>
<td>GEE</td>
<td>SPE</td>
<td>EE</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>----</td>
</tr>
<tr>
<td>*.rr</td>
<td>Configures attribute value pools.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>*.pro</td>
<td>Configures proxy realms.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>access.ini</td>
<td>Maps user or group account levels to administrative permissions. Used with admin.ini to grant administrators access privileges to administrative objects and actions.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>account.ini</td>
<td>Controls how RADIUS accounting attributes are logged.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>admin.ini</td>
<td>Maps administrative access levels to sets of access rights. Used with access.ini to grant administrators access privileges to administrative objects and actions.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>authlog.ini</td>
<td>Controls how RADIUS authentication requests are logged by Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>authReport.ini</td>
<td>Controls what authentication logs Steel-Belted Radius generates.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>authReportAccept.ini</td>
<td>Controls options for the acceptance authentication log file.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>authReportBadSharedSecret.ini</td>
<td>Controls options for the invalid shared secret authentication log file.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>authReportReject.ini</td>
<td>Controls options for the rejection authentication log file.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>authReportUnknownClient.ini</td>
<td>Controls options for the unknown client authentication log file.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>blacklist.ini</td>
<td>Configures blacklist settings, which are used to block authentication requests that match a blacklist profile.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>bounce.ini</td>
<td>Configures the auto-restart function for the Windows version of Steel-Belted Radius, which causes Steel-Belted Radius to restart itself automatically whenever it experiences a shutdown.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>ccagw.ini</td>
<td>Configures support for 3Com CCA tunnel attributes.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Table 3: Steel-Belted Radius Configuration Files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Function</th>
<th>GEE</th>
<th>SPE</th>
<th>EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>classmap.ini</td>
<td>Specifies what Steel-Belted Radius does with RADIUS attributes encoded in one or more Class attributes included in accounting requests.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>dhcp.ini</td>
<td>Configures DHCP address pools so that IP addresses can be assigned from a backend DHCP server.</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eap.ini</td>
<td>Configures EAP authentication methods used by Steel-Belted Radius.</td>
<td>x</td>
<td>SPE + EAP</td>
<td>x</td>
</tr>
<tr>
<td>events.ini</td>
<td>Controls dilutions and thresholds for Steel-Belted Radius events used to signal failures and warnings.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>fastauth.aut</td>
<td>Configures the EAP-FAST authentication method.</td>
<td>x</td>
<td>SPE + EAP</td>
<td>x</td>
</tr>
<tr>
<td>filter.ini</td>
<td>Sets up rules for filtering attributes into and out of RADIUS packets.</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldapauth.aut</td>
<td>Specifies settings for LDAP authentication in Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>lockout.ini</td>
<td>Configures settings that lock user accounts after repeated failed login attempts.</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>peapauth.aut</td>
<td>Configures the EAP-PEAP authentication method.</td>
<td>x</td>
<td>SPE + EAP</td>
<td>x*</td>
</tr>
<tr>
<td>proxy.ini</td>
<td>Stores information that applies to all realms on the server.</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>proxyrl.ini</td>
<td>Configures list of realms for forwarding accounting packets.</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>radius.ini</td>
<td>Configures a variety of operational settings for Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>radsql.acc</td>
<td>(Solaris/Linux only) Configures Oracle SQL accounting for the Solaris/Linux version of Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>radsql.aut</td>
<td>(Solaris/Linux only) Configures Oracle SQL authentication for the Solaris/Linux version of Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
</tbody>
</table>
### Table 3: Steel-Belted Radius Configuration Files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Function</th>
<th>GEE</th>
<th>SPE</th>
<th>EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>radsqljdbc.acc</td>
<td>(Solaris/Linux only) Configures JDBC SQL accounting for the Solaris/Linux version of Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>radsqljdbc.aut</td>
<td>(Solaris/Linux only) Configures JDBC SQL authentication for the Solaris/Linux version of Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>redirect.ini</td>
<td>Configures settings that redirect users after repeated failed login attempts.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>securid.ini</td>
<td>Specifies the prompt strings returned to RSA SecurID users during login and authentication.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>securidauth.aut</td>
<td>Configures the SecurID authentication method.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>servtype.ini</td>
<td>Configures service type mappings, which allow a user to have multiple authorization attribute sets based on the service type the user is requesting.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>sidalt.aut</td>
<td>Configures token caching for RSA SecurID authentication.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>spi.ini</td>
<td>Defines encryption keys and identifies the servers from which Steel-Belted Radius processes encrypted Class attributes in accounting requests.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>sqlacct.acc</td>
<td>(Windows only) Configures SQL accounting for the Windows version of Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>sqlauth.aut</td>
<td>(Windows only) Configures SQL authentication for the Windows version of Steel-Belted Radius.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>tacplus.ini</td>
<td>Specifies the name of the TACACS + server and the shared secret used to validate communication between the Steel-Belted Radius server and the TACACS + server.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>tlsauth.aut</td>
<td>Configures the TLS authentication method.</td>
<td>x</td>
<td>SPE + EAP</td>
<td>x</td>
</tr>
<tr>
<td>tlsauth.eap</td>
<td>Configures the operation of the TLS helper method.</td>
<td>x</td>
<td>SPE + EAP</td>
<td>x</td>
</tr>
<tr>
<td>ttlsauth.aut</td>
<td>Configures the TTLS authentication method.</td>
<td>x</td>
<td>SPE + EAP</td>
<td>x*</td>
</tr>
</tbody>
</table>
Tips for Editing Configuration Files

When editing configuration files, observe the following guidelines:

- Configuration files are text files that you can edit using a standard text editor, such as Notepad on Windows and `gedit` on Linux. If you use a word processing application such as Microsoft Word to edit your configuration files, make sure that you save the modified file in ASCII text format.

- You should make a backup copy of your configuration files before you make any changes, so that you have a working archive copy in the event that you delete or misconfigure an important setting and want to revert to your previous configuration.

- You can enter comments in configuration files by starting the line containing the comment with a semicolon (`;`) as the first character of the line. To disable a setting, consider commenting it out (by putting a semicolon at the start of the line) instead of deleting it.

- Put comments on a separate line above or below configuration settings. You cannot include comments on the same line as a configuration setting.

Correct:

; Set to 0 on 5/30/2006
Session_Timeout = 0

Incorrect:

Session_Timeout = 0 ; Set to 0 on 5/30/2006

- The default configuration files provided with Steel-Belted Radius typically include section headers and settings that are commented out. In such cases, Steel-Belted Radius uses the value shown in the commented setting as the default, meaning that you do not need to change the setting if you want to use the default value.

Table 3: Steel-Belted Radius Configuration Files (continued)

<table>
<thead>
<tr>
<th>File</th>
<th>Function</th>
<th>GEE</th>
<th>SPE</th>
<th>EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>uniport.aut</td>
<td>Configures the UniPort authentication method.</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>update.ini</td>
<td>Controls what information is updated when Steel-Belted Radius receives a HUP or USR2 signal.</td>
<td>x*</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>vendor.ini</td>
<td>Maps vendor-specific dictionary files to identifiers used in the Steel-Belted Radius administrative database.</td>
<td>x</td>
<td>x</td>
<td>x*</td>
</tr>
<tr>
<td>winauth.aut</td>
<td>Configures the WinAuth authentication method.</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
To change the value for a setting to something other than the default value, you must uncomment the setting by removing the semicolon at the start of the line. Note that the section headers (in square brackets) must also be uncommented for settings to be processed correctly.

- Make sure that lines containing settings or section headers have a text character in the first column. If a line has white space in the first column, it might not be processed correctly.

- You can edit configuration files while Steel-Belted Radius is running. However, changes to some files, such as `radius.ini`, require that you restart Steel-Belted Radius for the changes to take effect.
Chapter 2

Operations Files

This chapter describes the usage and settings for files used in Steel-Belted Radius operations and administration.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>access.ini File</td>
<td>8</td>
</tr>
<tr>
<td>admin.ini File</td>
<td>10</td>
</tr>
<tr>
<td>bounce.ini File (Windows only)</td>
<td>15</td>
</tr>
<tr>
<td>ccagw.ini File</td>
<td>17</td>
</tr>
<tr>
<td>eval.ini File</td>
<td>18</td>
</tr>
<tr>
<td>events.ini File</td>
<td>19</td>
</tr>
<tr>
<td>radius.ini File</td>
<td>22</td>
</tr>
<tr>
<td>sbrd.conf File (Solaris/Linux only)</td>
<td>50</td>
</tr>
<tr>
<td>services File</td>
<td>53</td>
</tr>
<tr>
<td>servtype.ini File</td>
<td>55</td>
</tr>
<tr>
<td>update.ini File</td>
<td>58</td>
</tr>
<tr>
<td>Auto-Restart Files (Solaris/Linux only)</td>
<td>62</td>
</tr>
</tbody>
</table>
access.ini File

Used by: GEE, SPE, SPE + MIM, SPE + EAP  
Not used by: EE

The access.ini file maps operating system user or group account names to levels of administrative privilege. The user account name and password used by an administrator when interacting with the Steel-Belted Radius server is granted access privileges according to the settings in this file.

[Settings] Section

The [Settings] section of access.ini contains overall configuration parameters; do not edit this section.

[Users] and [Groups] Sections

The syntax for the [Users] and [Groups] sections of the access.ini file (Table 4) is as follows:

```
[Users]  
UserName = AccessLevel  
_system.localhost = SnmpAgent  

[Groups]  
GroupName = AccessLevel  
```

NOTE: If you use SNMP to monitor your Steel-Belted Radius server, the [Users] section of your access.ini file must contain the following entry:

```
_system.localhost = SnmpAgent
```

If you are not using SNMP, you should comment out or delete the _system.localhost = SnmpAgent entry as a security precaution.

Table 4: access.ini Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserName</td>
<td>Each UserName or GroupName is the name of an authorized administrator account on the server. Depending on your platform, UserName and GroupName refer to a Windows domain user/group or a Solaris/Linux /etc/passwd user/group. You must list user accounts in the [Users] section and group accounts in the [Groups] section. You should list groups in priority order; rights are granted based on the first group found of which the user is a member.</td>
</tr>
<tr>
<td>GroupName</td>
<td></td>
</tr>
</tbody>
</table>
A special access level called **SuperAdmin** grants read/write access to all types of administrative data. This access level is always defined, and can be assigned to a user or group account in `access.ini` without appearing in `admin.ini`.

---

**Table 4: access.ini Syntax (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessLevel</td>
<td>The <code>AccessLevel</code> in each <code>access.ini</code> entry is the access level that you want to assign to that account. Each <code>AccessLevel</code> string must match the name of an <code>AccessLevel</code> section in <code>admin.ini</code>. You can define as many <code>AccessLevel</code> sections as you require. Once an <code>AccessLevel</code> section is defined in <code>admin.ini</code>, you can use <code>access.ini</code> to assign the access privileges associated with that level to users and group accounts.</td>
</tr>
</tbody>
</table>
admin.ini File

Used by: GEE, SPE, SPE + MIM, SPE + EAP
Not used by: EE

The admin.ini file maps administrative access levels to sets of access rights. These access levels are enforced for administrators connecting to Steel-Belted Radius by means of the SBR Administrator or the LDAP configuration interface (LCI). Each [AccessLevel] section in the admin.ini file corresponds to an AccessLevel name entered in the access.ini file. You can create as many [AccessLevel] sections in the admin.ini file as you require.

Access rights are defined according to the categories of administrative data that an account is allowed to read and/or write. These data categories correspond to SBR Administrator panels and to objects directly under o=radius in the LDAP configuration schema.

**NOTE:** If you omit a keyword, access to that data category is specifically denied for all information and windows that correspond to that keyword. Misspelled keywords are considered omitted.

**[AccessLevel] Section**

The syntax for each [AccessLevel] section (Table 5) defined in admin.ini is as follows:

```ini
[AccessLevel]
Access = value
Certificates = value
CCMPublish = value
CCMServerList = value
Configuration = value
CurrentUsers = value
ImportExport = value
IP-Pools = value
IPX-Pools = value
License = value
Profiles = value
Proxy = value
RAS-Clients = value
Report = value
RuleSets = value
Statistics = value
Tunnels = value
Users = value
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessLevel</td>
<td>Specifies the name of the access level. The value used here must be identical to the value used in the access.ini file.</td>
</tr>
</tbody>
</table>
Table 5: admin.ini Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Access      | Specifies whether administrators with this access level can read or write (update) administrative access data, which is controlled by the Administrators panel. Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access  
NOTE: When an administrator requests access, Steel-Belted Radius checks entries in the Administrators panel in SBR Administrator before checking the access.ini and admin.ini files. If an applicable administrative account exists in the Administrators panel, the user is given full access to the Steel-Belted Radius database, regardless of the configuration of the access.ini and admin.ini files. |
| Certificates | Specifies whether administrators with this access level can modify trusted root and server certificate information through the SBR Administrator. Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| CCMPublish  | Specifies whether administrators with this access level can publish server replication (ccmpkg) information through the SBR Administrator. Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| CCMServerList | Specifies whether administrators with this access level can read or write (update) information in the Replication panel in the SBR Administrator. Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| Configuration | Specifies whether administrators with this access level can read or write (update) information found in the Authentication Policies panel in the SBR Administrator. Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| CurrentUsers | Specifies whether administrators with this access level can read or write (update) the Current Sessions Table, which can be displayed in the Reports panel of SBR Administrator. Write access allows the administrator to delete entries from the Current Sessions Table. Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
<th>Details</th>
</tr>
</thead>
</table>
| ImportExport | Controls whether the Import and/or Export menu items are enabled in the SBR Administrator. | Valid values are:  
- r – Read-only access (allows export but not import)  
- w – Write-only access (allows import but not export)  
- rw – Read/write access (allows import and export)  
Data categories without read access are disabled. If a user tries to export categories of data without having sufficient access rights, categories for which the user does not have read access are omitted from the export operation. Similarly, if a user tries to import categories of data without having sufficient access rights, categories for which the user does not have write access are omitted from the import operation. **NOTE:** Import and Export are subject to the particular rights that the user has to each type of item, such as Users or Tunnels. |
| IP-Pools     | Specifies whether administrators with this access level can read or write (update) IP address pool data. Valid values are: | Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| IPX-Pools    | Specifies whether administrators with this access level can read or write (update) IPX address pool data. Valid values are: | Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| License      | Specifies whether administrators with this access level can add a new license. Valid values are: | Valid values are:  
- w – Write-only access  
- rw – Read/write access |
| Profiles     | Specifies whether administrators with this access level can read or write (update) profile data. Valid values are: | Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| Proxy        | Specifies whether administrators with this access level can read or write (update) proxy target data. Valid values are: | Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
| RAS-Clients  | Specifies whether administrators with this access level can read or write (update) RADIUS client data. Valid values are: | Valid values are:  
- r – Read-only access  
- w – Write-only access  
- rw – Read/write access |
[SNMPAgent] Section (GEE/SPE only)

If you use SNMP to monitor your Steel-Belted Radius server, the [SNMPAgent] section of admin.ini file must include the following section to give Read access to the SNMP agent.

```
[SnmpAgent]
RAS-Clients=r
Users=r
Profiles=r
Proxy=r
Tunnels=r
IP-Pools=r
IPX-Pools=r
Access=r
Configuration=r
Statistics=r
CurrentUsers=r
Report=r
ImportExport=r
```
bounce.ini File (Windows only)

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP
**Not used by:** EE

The bounce.ini configuration file enables and configures the Steel-Belted Radius auto-restart feature. This feature causes Steel-Belted Radius to restart itself automatically whenever it experiences a shutdown.

If you enable the auto-restart feature, it results in the loading of two copies of the server executable, `radius.exe`. After the parent executable is run, the parent executable runs the child executable. The parent periodically sends a message to the child to see if it is still operating. If the child does not respond to the message within 60 seconds (a configurable time period), the parent terminates the child, waits for a configurable number of seconds to allow `radius.exe` to fully shut down, and then starts a new copy of the child.

**NOTE:** When auto-restart is enabled and the server is running normally, you typically see two instances of `radius.exe` in any tool (such as the Task Manager) that you use to monitor processes on the Windows host computer.

While auto-restart is enabled, all server startup and shutdown activity is logged to a file called `bounce.log` in the server directory. Other types of server activity continue to be logged to the server log file (`yyyymmdd.log`) in the server directory.

**[Settings] Section**

The bounce.ini file contains one configuration section called `[Settings]` (Table 6).

```
[Settings]
Enable=1
MaxPong=25
MaxStartup=60
MaxShutDown=60
PingInterval=10
```

You should generally use the default values provided in the bounce.ini file. If you change any values, the MaxPong value should be greater than or equal to the PingInterval.

**Table 6: bounce.ini [Settings] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable     | ■ If set to 1, the auto-restart feature is enabled.  
            | ■ If set to 0, the auto-restart feature is disabled and other settings in the bounce.ini file are ignored.  
            | Default value is 0. |
Table 6: bounce.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxPong</td>
<td>Specifies the number of seconds that the parent waits for a response message from the child, before it decides the child is no longer operating and attempts to restart it. Default value is 25 seconds.</td>
</tr>
<tr>
<td>MaxShutdown</td>
<td>Specifies the number of seconds that the parent allows for normal shutdown of the child. If the child does not terminate within that time, the parent terminates the child. Default value is 60 seconds.</td>
</tr>
<tr>
<td>MaxStartup</td>
<td>Specifies the number of seconds that the parent allows for starting up the child. If the child does not send a message within that time, the parent decides the startup was not successful and exits. Default value is 60 seconds.</td>
</tr>
<tr>
<td>PingInterval</td>
<td>Specifies the number of seconds between each message sent by the parent to the child to check whether it is running. Default value is 10 seconds.</td>
</tr>
</tbody>
</table>
ccagw.ini File

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE
Not used by: —

The ccagw.ini file contains information about 3COM CCA gateways. You must configure a [gateway] section for each 3COM CCA gateway to enable the return of required CCA tunnel attributes.

[gateway] section

Each [gateway] section of the ccagw.ini file (Table 7) contains information about a specific 3COM CCA gateway.

[Jupiter-Gateway]
Address = 200.47.98.142
TunnelRefresh = 3600
Description = Jersey City facility, East Coast subscribers
Secret = Holland Tunnel

Table 7: ccagw.ini [gateway] Section

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Specifies the IPv4 address of the gateway.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You cannot use IPv6 addresses with ccagw.ini.</td>
</tr>
<tr>
<td>TunnelRefresh</td>
<td>Specifies the number of seconds before the tunnel refreshes.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a text string describing the gateway.</td>
</tr>
<tr>
<td>Secret</td>
<td>Specifies the shared secret used to authenticate communication</td>
</tr>
<tr>
<td></td>
<td>between Steel-Belted Radius and the gateway device.</td>
</tr>
</tbody>
</table>
eval.ini File

**Used by:** GEE, SPE, EE  
**Not used by:** SPE + MIM, SPE + EAP

The eval.ini file contains temporary license key information for evaluation installations of Steel-Belted Radius. The eval.ini file does not contain any configurable settings.
events.ini File

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE
Not used by: —

The events.ini configuration file controls dilutions and thresholds for Steel-Belted Radius events that are used to communicate failures, warnings, and other information. Events are handled by the Windows Events Viewer.

Appendix D, “Windows Events,” summarizes common event values. Note that only some of these events support thresholds or dilution.

[EventDilutions] Section

The [EventDilutions] section of events.ini specifies how many events must occur before Steel-Belted Radius generates an event report. This feature lets you “dilute” the rate at which frequently occurring events are logged.

Syntax is as follows:

```
[EventDilutions]
EventName=DilutionCount
```

where EventName identifies a Steel-Belted Radius event and DilutionCount specifies how many times this event must occur before it is recorded in the Windows event log or to the SNMP manager program.

Example

The following example specifies that a Steel-Belted Radius server configured to authenticate against a SQL database reports every fifth SQLConnectFailure (warning event number 5008) error:

```
[EventDilutions]
; 5008 - nnnn attempts to connect to SQL server failed.
SQLConnectFailure=5
```

If an SQL error condition prevents the server from connecting to the database, Steel-Belted Radius retries the connection (and reports these attempts in the RADIUS log file yyyyymmdd.log). Steel-Belted Radius does not trigger warning event 5008 until the fifth connection attempt fails.

[Suppress] Section

The [Suppress] section of events.ini lets you suppress Steel-Belted Radius events. An event whose ID number (Windows) or trap number (Solaris/Linux) appears in this section is not reported when the applicable informational, warning, or error condition occurs.
**Example**

The following settings suppress events relating to verification server timeouts (5013) or failures (5014).

```
[Suppress]
5013
5014
```

**[Thresholds] Section**

The [Thresholds] section of `events.ini` (Table 8) lets you specify thresholds that trigger an event report. Thresholds often come in pairs, where a warning event is generated when a resource becomes scarce (low threshold is crossed), and an information event is generated when the resource becomes available (high threshold is crossed).

The [Thresholds] section lets you tune Steel-Belted Radius event generation for items such as system memory, thread count, and file system space, and can differ for each computer depending on resources, configuration, and other applications.

**Table 8: `events.ini` [Thresholds] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThreadAvailWarningIssue</td>
<td>When the number of available accounting or authentication threads reaches the specified value, issue the warning event <code>RADMSG_THREADS_LOW</code> or <code>funkSbrTrapLowThreads</code> (5001). Default value is 10.</td>
</tr>
<tr>
<td>ThreadAvailWarningClear</td>
<td>When the number of available accounting or authentication threads reaches the specified value, issue the informational event <code>RADMSG_THREADS_NORMAL</code> or <code>funkSbrTrapThreadsNormal</code> (102). Default value is 20.</td>
</tr>
<tr>
<td>FileSystemFreeKBWarningIssue</td>
<td>When available system disk space falls to the specified value, issue the warning event <code>RADMSG_FILE_SYSTEM_LOW</code> or <code>funkSbrTrapLowFSSpace</code> (5007). Default value is 4096 KB (4MB).</td>
</tr>
<tr>
<td>FileSystemFreeKBWarningClear</td>
<td>When the number of kilobytes of available system disk space reaches the specified value, issue the informational event <code>RADMSG_FILE_SYSTEM_NORMAL</code> or <code>funkSbrTrapFSNormal</code> (103). Default value is 8092 KB (8MB).</td>
</tr>
<tr>
<td>ReserveMemoryKB</td>
<td>Reserve this amount of memory (in kilobytes) at system startup for cases of overload. If a memory allocation failure occurs, Steel-Belted Radius frees the reserved memory and reports the event. Default value is 2048 KB (2MB).</td>
</tr>
<tr>
<td>PoolPctAddressAvailWarningIssue</td>
<td>When the number of available addresses in any IP address pool drops below the specified percentage, issue a <code>funkSbrTrapIPAddrPoolLow</code> warning. Default value is 20 percent.</td>
</tr>
</tbody>
</table>
**Table 8: events.ini [Thresholds] Syntax (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| PoolPctAddressAvailWarningClear                | When the number of available addresses in any IP address pool rises above the specified percentage, issue an informational message.  
|                                                | Default value is 40 percent.                                              |

**Example**

This following example would produce a warning event (5001) when the number of available accounting or authentication threads falls below 10 percent, and an informational event (102) is issued when it rises above 20 percent.

```
[Thresholds]
ThreadAvailWarningIssue=10
ThreadAvailWarningClear=20
```
radius.ini File

Used by: GEE, SPE*, SPE + MIM, SPE + EAP, EE*
Not used by: —

The radius.ini initialization file is the main configuration file that determines the operation of Steel-Belted Radius. It contains information that controls a variety of Steel-Belted Radius functions and operations.

[Addresses] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE*
Not used by: —

By default, the Steel-Belted Radius server tries to autoconfigure all IPv4 addresses that are reported by name services for the primary host name of the server on which Steel-Belted Radius is running, so that it can listen for incoming RADIUS packets on all available network interfaces. If IPv6 is enabled, Steel-Belted Radius autoconfigures its IPv6 addresses and then listens on all interfaces using IPv6 addresses.

You should explicitly configure the IP addresses that you want Steel-Belted Radius to use in the [Addresses] section of radius.ini if Steel-Belted Radius is running on a multi-homed (more than one network interface) server and if any of the following statements apply to your network:

- One or more network interfaces on the server are connected to networks that should not carry RADIUS traffic.
- The server has more than one host name, and IP addresses exist for names other than the primary host name.
- The server has private IP addresses that are not published by name services.

Specifying IPv4 or IPv6 addresses causes the server to listen on only those addresses and ignore all other addresses.

Specifying AutoConfigureIPv4 or AutoConfigureIPv6 causes Steel-Belted Radius to attempt to discover and configure all IPv4 or IPv6 addresses that belong to the local host automatically.

Example 1

The following example configures Steel-Belted Radius to listen for RADIUS authentication and accounting requests on the IPv4 address 192.168.12.35 and on all local IPv6 interfaces. Note that IPv6 functionality must be enabled (by setting Enable to 1 in the [IPv6] section of radius.ini) before IPv6 addresses can be used.

[Addresses]
192.168.12.35
AutoConfigureIPv6
To route all of your proxy traffic through a single interface, set the value for `ProxySource` in the [Configuration] section of `radius.ini` to the appropriate IP address or addresses, which must be listed in the [Addresses] section.

**Example 2**

The following example routes all proxy traffic through the interface at 192.10.20.30:

```
[Addresses]
192.10.20.30
192.10.20.31

[Configuration]
ProxySource = 192.10.20.30
```

**GEE/SPE:** The `ProxySource` setting in the [Configuration] section of `radius.ini` disables per-realm control of proxy outbound interfaces. If `ProxySource` is not set, sockets are opened and bound for each interface on the server. To route different proxy realms through specific interfaces using the `proxy.ini` file, refer to “[Interfaces] Section” on page 162.

**[AuditLog] Section**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not used by:** —

The [AuditLog] section (Table 9) specifies whether Steel-Belted Radius maintains an audit log file (`yyyymmdd.auditlog`) to record administrator activities and CCM events. Audit log records are stored in XML format.

Administrator activities include the following:

- Logging in and out by Steel-Belted Radius administrators
- Creating, modifying, and deleting Steel-Belted Radius objects (RADIUS clients, users, profiles, proxy targets, proxy realms, tunnels, administrators, authentication policies, or CCM nodes)
- Importing files

CCM events include publication, notification, and download of CCM files.

**NOTE:** The audit log does not track changes made through the LDAP configuration interface (LCI).

```
[AuditLog]
;Enable = 0
;LogfilePermissions = owner:group mode
;DaysToKeep = 30
```
You configure the [AuthRejectLog] section of radius.ini (Table 10) to specify what types of authentication method rejection messages Steel-Belted Radius records in the RADIUS log file (yyyymmdd.log). You can specify that you want the server log file to record reject information generated by all authentication methods, reject information of one or more specific types, or the most relevant rejection information.

Processing an authentication request might result in multiple instances of an authentication method being given a chance to authenticate the user. If this occurs and at least one authentication method succeeds in authenticating the user, no messages are recorded to the server log file. If this occurs and all instances fail to authenticate the user, you can specify that only the most relevant reason for the authentication failure is recorded. For example, if one method resulted in an authentication error of type InvalidCredentials and another results in an authentication error of type SystemError, only the InvalidCredentials message would be logged.

You can specify that more than one type of log message should be recorded by entering more than one filter type value for the Filter parameter.
Table 10: radius.ini [AuthRejectLog] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>If set to 0, authentication reject details are not recorded in the server log file. If set to 1, authentication reject details of the specified type(s) are recorded in the server log file. Default value is 0.</td>
</tr>
<tr>
<td>Filter</td>
<td>Specifies the types of authentication reject messages to be recorded: ▪ <strong>All</strong> – Record authentication rejection details from all authentication methods. ▪ <strong>MostRelevant</strong> – When multiple authentication methods are tried and all fail, record the most relevant error messages (the messages with the greatest severity). If two messages have the same severity, both are listed. The following values are listed in order of greatest to least relevance: ▪ <strong>PostProcessRejection</strong> – User was authenticated successfully but postprocessing caused rejection. ▪ <strong>InvalidCredentialsOrUser</strong> – User was not authenticated because user was not found or credentials were invalid. ▪ <strong>InvalidCredentials</strong> – User was not authenticated because user was known but the password or certificate was not correct. ▪ <strong>UnsupportedCredentialType</strong> – User was not authenticated because the credentials presented were of the wrong type. ▪ <strong>UserNotFound</strong> – User was not authenticated because user could not be found in the authentication database. ▪ <strong>AccessError</strong> – Authentication failed because a database or remote server was inaccessible. ▪ <strong>InvalidRequest</strong> – User was not authenticated because the request appeared to be malformed. ▪ <strong>BlacklistedUser</strong> – User was not authenticated because user is blacklisted. ▪ <strong>SystemError</strong> – User was not authenticated because of a system error such as a resource allocation error.</td>
</tr>
</tbody>
</table>

The following example would cause authentication reject details from all authentication methods to be recorded to the server log file.

```
[AuthRejectLog]
Enable = 1
Filter = All
```

The following example would cause all authentication reject details of type SystemError to be recorded.

```
[AuthRejectLog]
Enable = 1
Filter = SystemError
```
The following example would cause all authentication reject details of type SystemError, BlacklistedUser, or UserNotFound to be recorded.

```
[AuthRejectLog]
Enable = 1
Filter = SystemError, BlacklistedUser, UserNotFound
```

[Configuration] Section

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE*

**Not used by:** —

The [Configuration] section of `radius.ini` (Table 11) contains parameters that control basic behavior of Steel-Belted Radius.

**Table 11: radius.ini [Configuration] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AcctAutoStopEnable</td>
<td>The Proxy AutoStop feature forwards session termination information to downstream proxy RADIUS servers when a user session is closed, so that the resources associated with the user session can be freed.</td>
</tr>
<tr>
<td></td>
<td>- If set to 0, the Proxy AutoStop feature is disabled.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, the Proxy AutoStop feature is enabled.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>AddDestIPAddressAttrToRequest</td>
<td>If set to 0, Steel-Belted Radius does not add destination address information to RADIUS requests.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, Steel-Belted Radius adds a Funk-Dest-IP-Address attribute identifying the IP address to which the RADIUS request was sent to the attributes in the packet. All processing that could be performed on an attribute included in the request packet, such as checklist processing, can be performed on this attribute.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>GEE/SPE:</strong> If you enable this attribute, the attribute is visible to the proxy module. If your environment proxies requests, you might want to configure Steel-Belted Radius to strip the attribute from the request before forwarding the request to a downstream server.</td>
</tr>
</tbody>
</table>
Table 11: radius.ini [Configuration] Syntax  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddDestUDPPortAttrToRequest</td>
<td>- If set to 0, Steel-Belted Radius does not add destination port information to RADIUS requests.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, Steel-Belted Radius adds a Funk-Dest-UDP-Port attribute identifying the UDP port to which the RADIUS request was sent to the attributes in the packet. All processing that could be performed on an attribute included in the request packet, such as checklist processing, can be performed on this attribute. Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>GEE/SPE:</strong> If you enable this attribute, the attribute is visible to the proxy module. If your environment proxies requests, you might want to configure Steel-Belted Radius to strip the attribute from the request before forwarding the request to a downstream server.</td>
</tr>
<tr>
<td>AddFunkClientGroupToRequest</td>
<td>- If set to 0, Steel-Belted Radius does not add a Funk-Radius-Client-Group attribute to an incoming RADIUS request.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, Steel-Belted Radius adds a Funk-Radius-Client-Group attribute to the RADIUS request. The value of the Funk-Radius-Client-Group attribute is set to the name of the client group. Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You should enable this option only if you configure RADIUS client groups in SBR Administrator. For more information on RADIUS client groups, refer to the <em>Steel-Belted Radius Administration Guide</em>.</td>
</tr>
<tr>
<td>AddFunkLocationGroupIdToRequest</td>
<td>- If set to 0, Steel-Belted Radius does not add a Funk-Location-Group-Id attribute to an incoming RADIUS request.</td>
</tr>
<tr>
<td>(GEE/SPE only)</td>
<td>- If set to 1, Steel-Belted Radius adds a Funk-Location-Group-Id attribute to an incoming RADIUS request if the request comes from a client in a configured location group. The value of the Funk-Location-Group-Id attribute is set to the name of the location group, which can be used for SQL, LDAP, and checklist processing. Default value is 0.</td>
</tr>
</tbody>
</table>
Table 11: radius.ini [Configuration] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| AddSourceIPAddressAttrToRequest  | - If set to 0, Steel-Belted Radius does not add source address information to RADIUS requests.  
|                                  | - If set to 1, Steel-Belted Radius adds a Funk-Source-IP-Address attribute identifying the IP address from which the RADIUS request was received to the attributes in the packet. All processing that could be performed on an attribute included in the request packet, such as checklist processing, can be performed on this attribute.  
|                                  | Default value is 0.  
|                                  | **GEE/SPE:** If you enable this attribute, the attribute is visible to the proxy module. If your environment proxies requests, you might want to configure Steel-Belted Radius to strip the attribute from the request before forwarding the request to a downstream server. |
|                                |  
| Apply-Login-Limits               | - If set to yes, the maximum number of concurrent connections for each user is enforced, and connection attempts above the limit are rejected.  
|                                | - If set to no, connections above the limit are allowed, but an event is noted in the server log file.  
|                                | Default value is yes.  
|                                |  
| AttributeEdit                    | - If set to 1, the attribute editing feature for proxy realms is enabled.  
| (GEE/SPE only)                   | - If set to 0, the feature is disabled.  
|                                | Default value is 1.  
|                                |  
| AuthenticateOnly                 | - If set to 1, no response attributes are included in the response packet to an AuthenticateOnly (Service-Type 8) request.  
|                                | - If set to 0, the normal response attributes are included in the response.  
|                                | Default value is 1.  
|                                |  
| AutoPasswords                    | If set to yes, support for SHA and UNIXcrypt passwords for authentication against the native database are enabled.  
| (GEE/SPE only)                   | Default value is no (disabled).  
|                                |  
| CheckMessageAuthenticator        | Specifies whether validation of Message-Authenticator occurs on receipt of an Access-Request from a network access device or on receipt of an Access-Accept, Access-Reject, or Access-Challenge from a proxy (extended proxy only).  
|                                | - If set to 0, the validation of received Message-Authenticator attributes is disabled.  
|                                | - If set to 1, the validation of received Message-Authenticator attributes is enabled.  
|                                | Default value is 0.  
|                                | **NOTE:** Validation does not occur for ordinary proxy.  
|
### Table 11: radius.ini [Configuration] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| **ClassAttributeStyle** | If set to 1, Steel-Belted Radius uses unencrypted Class attributes with multiple ASCII keys in Access-Accept packets.  
If set to 2, Steel-Belted Radius uses enhanced/encrypted Class attributes in Access-Accept packets.  
Default value is 2.  
**NOTE:** The ClassAttributeStyle parameter must be set to a value of 2 before you can use attribute embedding. For information on attribute embedding, see “[Debug] Section” on page 35. |
| **DisableSecondaryMakeModelSelection** | If set to 1, Steel-Belted Radius looks up the network access device entry by using the source address of the request and sets the make/model according to the information specified for the client.  
If set to 0, Steel-Belted Radius:  
1. Looks up the network access device entry by using the source address of the request and sets the make/model according to the information specified for the client.  
2. Uses the NAS-IP-Address attribute (if present) to look up the network access device entry. If the IP address is found, override the make/model information identified in Step 1.  
3. Uses the NAS-Identifier attribute (if present) to look up the network access device by name. If the name is found, override the make/model information defined in Step 1 or Step 2.  
Default value is 0. |
| **EnableEricssonViGHTTPDigestSupport** | If set to 1, the Ericsson ViG version of HTTP Digest Access authentication is enabled.  
If set to 0, the Ericsson ViG version of HTTP Digest Access authentication is disabled.  
When the Ericsson ViG version of HTTP Digest Access authentication is enabled, Steel-Belted Radius looks for the ViG VSAs when it parses incoming packets, and, if it finds them, converts them to AVPs compatible with the current HTTP Digest Access authentication.  
Default value is 0.  
**NOTE:** This setting is ignored if the EnableHTTPDigestSupport setting is set to 0 (disabled). |
| **EnableHTTPDigestSupport** | If set to 1, HTTP Digest Access authentication is enabled.  
If set to 0, HTTP Digest Access authentication is enabled.  
When HTTP Digest Access authentication is enabled, Steel-Belted Radius interprets the inclusion of certain attribute-value pairs in an Access-Request message as a request to use HTTP Digest Access authentication.  
Default value is 0. |
### Table 11: radius.ini [Configuration] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| EnhancedDiagnosticLogging | - If set to no, standard diagnostic logging messages are written to the RADIUS log file when the log level is set to 0.  
                             - If set to yes, messages relating to proxy retries, proxy timeouts, and LDAP timeouts, as well as standard diagnostic logging messages, are written to the RADIUS log file (yyyyymmdd.log) when the log level is set to 0.  
                             Default value is no.                                                                                                                              |
| ExtendedProxy (GEE/SPE only) | - If set to 1, you can set up realms for proxy RADIUS or directed authentication/accounting  
                             - If set to 0, Steel-Belted Radius can proxy-forward to specific servers (identified using Proxy entries in the Administrator program), but proxy realms and directed realms are disabled.  
                             If the ExtendedProxy setting is not present in the [Configuration] section, realms are disabled by default.  
                             Default value is 1.                                                                                                                             |
| FramedIPAddressHint       | If set to yes, the attribute Framed-IP-Address is treated as a hint. If this attribute appears in the Access-Request and the user’s return list is configured to allocate Framed-IP-Address from a pool, the IP address in the Access-Request is returned instead of a newly-allocated IP address.  
                             Default value is no.                                                                                                                             |
| LogAccept                 | - If set to 1, specifies that messages associated with Accepts that meet the current LogLevel should be recorded in the server log file.  
                             - If set to 0, messages associated with Accepts are ignored.  
                             Default value is 1.  
                             **GEE/SPE:** The LogReject setting is re-read whenever the server receives a HUP signal.  
                             **GEE/SPE:** The LogAccept setting is re-read whenever the server receives a HUP signal.                                                |
| LogDir (GEE/SPE only)     | Sets the destination directory on the local host where server log files are stored.  
                             Default value is the Steel-Belted Radius directory.  
                             **NOTE:** You cannot write server log files to a mapped or shared drive.                                                                    |
Table 11: radius.ini [Configuration] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| LogFilePermissions               | Specifies the owner and access permission setting for the system log (yyyymmdd.log) file. Enter a value for the LogFilePermissions setting in owner:group permissions format, where:  
  - **owner** specifies the owner of the file in text or numeric format.  
  - **group** specifies the group setting for the file in text or numeric format.  
  - **permissions** specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format.  
  For example, ralphw:1007 rw- - - - - specifies that the file owner (ralphw) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and other users cannot access the log file. |
| LogfileMaxMBytes                 | If set to 0 (or if setting is absent), the server log file size is ignored and log file names are date-stamped to identify when they were opened (yyyymmdd.log).  
  If set to a value in the range 1-2047, the current server log file is closed when it reaches the specified number of megabytes (1024 x 1024 bytes), and a new server log file using the date and time it was opened as its filename (yyyymmdd_hhmm.log) is opened.  
  Default value is 0.  
  **NOTE:** The size of the log file is checked once per minute. The log file might exceed the size specified in LogFileMaxMBytes, since it does not roll over until the next log size check occurs. |
| LogHighResolutionTime            | If set to no, the timestamp for entries in the Steel-Belted Radius log file (yyyymmdd.log) are recorded as hh:mm:ss (hours:minutes:seconds).  
  If set to yes, the timestamp for entries in the Steel-Belted Radius log file (yyyymmdd.log) are recorded as hh:mm:ss:xxx, where xxx represents the number of elapsed milliseconds since the ss value changed.  
  Default value is no. |
| LogLevel                         | Sets the rate at which Steel-Belted Radius writes entries to the server log file (.LOG):  
  - 0 – Production logging level  
  - 1 – Informational logging level  
  - 2 – Debug logging level  
  Default value is 0.  
  **GEE/SPE:** The LogLevel setting is re-read whenever the server receives a HUP signal. |
### Table 11: radius.ini [Configuration] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogReject</td>
<td>- If set to 0, messages associated with Rejects are ignored.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, messages associated with Rejects that meet the current LogLevel should be recorded in the server log file. Default value is 1.</td>
</tr>
<tr>
<td></td>
<td><strong>GEE/SPE:</strong> The LogReject setting is re-read whenever the server receives a HUP signal.</td>
</tr>
<tr>
<td>NoNullTermination</td>
<td>- If set to 0, RADIUS reply attributes of type <code>string</code> are sent with a null character at the end of the string (null terminated string).</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, RADIUS reply attributes of type <code>string</code> are sent without the null character at the end of the string. Entering a value of 1 for this setting is the equivalent of changing all reply attributes of type <code>string</code> to type <code>stringnz</code>. Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> After you change this setting, you must delete the <code>savedicts.bin</code> file and restart the Steel-Belted Radius service.</td>
</tr>
<tr>
<td>PhantomTimeout</td>
<td>The maximum number of seconds that a phantom session record remains active. As soon as the corresponding accounting start packet is received, a phantom record is discarded. If a phantom record still exists at the end of its timeout period, it is discarded and all resources associated with it are released.</td>
</tr>
<tr>
<td>PrivateDir</td>
<td>Name of the location of the Steel-Belted Radius directory, which contains the database and dictionary files. Default value is the directory in which the Steel-Belted Radius service/daemon resides.</td>
</tr>
<tr>
<td>ProcessRealmBeforeTunnel (GEE/SPE only)</td>
<td>- If set to 0, Steel-Belted Radius checks whether a request matches the criteria established for tunnels before it tests whether a request matches the criteria for proxy and directed realms.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, Steel-Belted Radius checks whether a request matches the criteria established for proxy and directed realms before it tests whether a request matches the criteria established for tunnels. Default value is 0.</td>
</tr>
<tr>
<td>ProxyFastFail (GEE/SPE only)</td>
<td>Specifies the number of seconds a Steel-Belted Radius server continues to forward packets to a proxy RADIUS target that appears to be down. A value of 0 disables the feature. Default value is 300.</td>
</tr>
</tbody>
</table>
## Table 11: radius.ini [Configuration] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProxySource</td>
<td>Specifies the IP address of the interface through which all outgoing proxy traffic is routed. The IP address specified for ProxySource must be listed in the [Addresses] section of radius.ini. If a ProxySource address is not specified and per-realm control of proxy interfaces is not enabled, Steel-Belted Radius uses the first interface it finds on the server.</td>
</tr>
</tbody>
</table>
| ProxyStripRealm           | ● If set to 1, the proxy realm decoration is stripped before sending the request downstream.  
                               ● If set to 0, no realm name stripping is performed.  
                               Default value is 1.                                      |
| SelectIPPoolNameByNasAVPs | ● If set to 0, the IP address pool for a RADIUS client is based on the source IP address in the UDP packet containing the access request.  
                               ● If set to 1, the IP address pool for a RADIUS client is based on the value of the NAS-IP-Address or NAS-Identifier attribute included in the access request. If the NAS-IP-Address or NAS-Identifier attribute is not present, or if a RADIUS client matching the IP address or identifier cannot be found, the IP address pool for a RADIUS client is based on the source IP address in the UDP packet containing the access request.  
                               Default value is 0.                                      |
When a user’s identity information is encrypted during authentication, Steel-Belted Radius uses a special Class attribute to pass the user’s encrypted identity to an accounting server. Because this typically requires more than one Class attribute to be included in the Accept response, and because some Access Points do not support echoing more than one Class attribute, you can use the SendOnlyOneClassAttribute parameter to specify how Steel-Belted Radius should forward encrypted user identity information.

- If set to 1, Steel-Belted Radius creates a Class attribute containing a Class attribute flag, a server identifier, and a transaction identifier. The user identification data that would normally be stored in the Class attribute(s) is stored in the current sessions table. When Steel-Belted Radius receives an accounting request, it looks up the Class information in the current sessions table and uses it as if it had arrived in the accounting request packet.

- If set to 0, Steel-Belted Radius creates one or more Class attributes to return a user’s encrypted identity to the Access Point, with the assumption that the AP forwards the Class attribute(s) containing the encrypted user identification information to the accounting server.

Default value is 0.

**NOTE:** This feature works only if accounting requests go to the same server that performs authentication. Accounting requests that go to servers other than the authenticating server fail.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SendOnlyOneClassAttribute</td>
<td>When a user’s identity information is encrypted during authentication, Steel-Belted Radius uses a special Class attribute to pass the user’s encrypted identity to an accounting server. Because this typically requires more than one Class attribute to be included in the Accept response, and because some Access Points do not support echoing more than one Class attribute, you can use the SendOnlyOneClassAttribute parameter to specify how Steel-Belted Radius should forward encrypted user identity information.</td>
</tr>
</tbody>
</table>

- If set to 1, Steel-Belted Radius creates a Class attribute containing a Class attribute flag, a server identifier, and a transaction identifier. The user identification data that would normally be stored in the Class attribute(s) is stored in the current sessions table. When Steel-Belted Radius receives an accounting request, it looks up the Class information in the current sessions table and uses it as if it had arrived in the accounting request packet.

- If set to 0, Steel-Belted Radius creates one or more Class attributes to return a user’s encrypted identity to the Access Point, with the assumption that the AP forwards the Class attribute(s) containing the encrypted user identification information to the accounting server.

Default value is 0.

**NOTE:** This feature works only if accounting requests go to the same server that performs authentication. Accounting requests that go to servers other than the authenticating server fail.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartupTimeout</td>
<td>Specifies the number of seconds Steel-Belted Radius waits for its startup sequence to finish before timing out. Default value is 360 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| TraceLevel        | Specifies the RADIUS packet tracing level:  
|                   | 0 – No packet tracing  
|                   | 1 – Parsed content of packets is logged  
|                   | 2 – Raw content and parsed content of the packet is logged  

Default value is 0.

**NOTE:** Packet traces are written to the server log file and can be a useful tool for troubleshooting interoperability problems.
Table 11: radius.ini [Configuration] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| TreatAddressPoolsAsDisjoint      | ■ If set to 1, Steel-Belted Radius treats each IP address pool as though it operates off its own disjoint address space. This disables the normal checks to ensure that an IP address is allocated only to a single address pool.  
  ■ If set to 0, a single IP address can be allocated only to a single session and from a single IP address pool.  
  Default value is 0.  
  NOTE: To track allocated resources, Steel-Belted Radius uses the Class attribute to track IP addresses. This attribute contains the IP pool name and IP address. |
| UseNewAttributeMerge             | ■ If set to 1, the new profile and user attribute merging calculation is performed.  
  ■ If set to 0, the older calculation technique is used.  
  Refer to “Resolving Profile and User Attributes” in the Steel-Belted Radius Administration Guide for an explanation of new attribute merging.  
  Default value is 1. |

[CurrentSessions] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE  
Not used by: —

The [CurrentSessions] section of radius.ini (Table 12) controls the Current Sessions Table.

[CurrentSessions]  
;CaseSensitiveUsernameCompare = 1

Table 12: radius.ini [CurrentSessions] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| CaseSensitiveUsernameCompare     | ■ If set to 1, when the server searches its Current Sessions Table for sessions that have the same username, it uses case-sensitive lookups.  
  ■ If set to 0, the server ignores case.  
  Default value is 1. |

[Debug] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE  
Not used by: —

The [Debug] section of radius.ini (Table 13) helps debug problems with Steel-Belted Radius operations by incorporating thread identifiers in log messages. Thread identifiers help you parse the diagnostic log when messages about different RADIUS requests are interleaved.
The syntax for including thread identifiers in diagnostic log messages is as follows:

```plaintext
[Debug]
Log-Thread-ID = yes
```

Table 13: radius.ini [Debug] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log-Thread-ID</td>
<td>If set to yes, thread identifiers are included in Steel-Belted Radius log messages.</td>
</tr>
<tr>
<td></td>
<td>If set to no, thread identifiers are omitted from Steel-Belted Radius log messages.</td>
</tr>
<tr>
<td></td>
<td>Default value is no.</td>
</tr>
</tbody>
</table>

**[EmbedInClass] Section**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not used by:** —

The [EmbedInClass] section of radius.ini (Table 14) identifies attributes that are available during authentication processing which must be made available in accounting requests. Attribute embedding allows billing information to be embedded in a Class attribute returned to Steel-Belted Radius by a network access device. When Steel-Belted Radius receives an embedded attribute, it decodes the attribute and places it in the Accounting request according to the settings specified in the classmap.ini file (described on page 117).

**NOTE:** The ClassAttributeStyle parameter in the [Configuration] section of radius.ini must be set to a value of 2 before you can use attribute embedding.

The syntax for embedding attributes is as follows:

```plaintext
[EmbedInClass]
responseAttribute={ Clear | Encrypt },[Remove]
```

Table 14: radius.ini [EmbedInClass] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>responseAttribute</td>
<td>Identifies the response attribute to be embedded in the RADIUS Class attribute.</td>
</tr>
<tr>
<td>Clear</td>
<td>Specifies that the retrieved information is included in the Class attribute in cleartext format.</td>
</tr>
<tr>
<td>Encrypt</td>
<td>Specifies that the retrieved information is encrypted before it is included in the Class attribute.</td>
</tr>
<tr>
<td>Remove</td>
<td>Optional parameter that removes the embedded attribute from the Accept-Response packet.</td>
</tr>
</tbody>
</table>

**[FailedAuthOriginStats] Section (Windows only)**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not used by:** —
The [FailedAuthOriginStats] section of radius.ini enables you to identify when a specific network access device is associated with certain Windows Performance Monitor (perfmon) counters. This helps you to identify a specific region of your network that might be having difficulties. The syntax is as follows:

```
[FailedAuthOriginStats]
RADIUSclient=IDnumber
RADIUSclient=IDnumber
...
```

where `RADIUSclient` is the name of a network access device as defined in the RADIUS Clients window, and `IDnumber` is a number in the range 1 to 16. These numbers map to the following Steel-Belted Radius perfmon counters:

- Failed Auths - 1
- Failed Auths - 2
- ...
- Failed Auths - 16

For example, if you map a RADIUS client named herman to the number 3, then the perfmon counter `Failed Auths - 3` tells you the number of failed authentication requests that have originated from RADIUS client herman.

```
[FailedAuthOriginStats]
herman=3
```

**[HiddenEAPIdentity] Section**

*Used by: GEE, SPE + EAP, EE*

*Not used by: SPE, SPE + MIM*

The [HiddenEAPIdentity] section of radius.ini allows the known inner identity of EAP/TTLS and EAP/SIM protocols to be included in the Access-Accept message returned in response to an authentication request.

The syntax is as follows:

```
[HiddenEAPIdentity]
IncludeInAcceptResponse=0|1
ResponseAttribute = attributeName[, replaceAttribute]
```

**Table 15: radius.ini [HiddenEAPIdentity] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>IncludeInAcceptResponse</td>
<td>- If set to 0, inclusion of the inner identity in Access-Accept responses is disabled.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, Steel-Belted Radius includes the inner identity in the specified attribute of an Access-Accept response. Default value is 0.</td>
</tr>
</tbody>
</table>
[IPPoolSuffixes] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP
Not used by: EE

The [IPPoolSuffixes] section of radius.ini lets you define suffixes that can be used to split the IP address pools reserved for a network access device into smaller subcategories.

The syntax is as follows:

```
[IPPoolSuffixes]
Suffix1
Suffix2
...
```

For example, to create three categories that append -Bronze, -Silver, and -Gold to IP Address Pool names, this section would be defined as follows:

```
[IPPoolSuffixes]
-Bronze
-Silver
-Gold
```

[IPv6] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE
Not used by: —

```
[IPv6]
Enable = 0
DynamicNameResolution = 2
IPv6LinkLocalUnicastScopeld = 0
IPv6SiteLocalUnicastScopeld = 0
```
The [IPv6] section of radius.ini (Table 16) controls IPv6 network transport features.

**Table 16: radius.ini [IPv6] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Determines whether IPv6 networking is enabled in Steel-Belted Radius.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, IPv6 networking is disabled, and other values in the IPv6 section of radius.ini are ignored.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, IPv6 networking is enabled.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> IPv4 networking is always enabled in Steel-Belted Radius.</td>
</tr>
<tr>
<td>DynamicNameResolution</td>
<td>Determines whether the Steel-Belted Radius server tries to use IPv6 name services (DNSv6) to resolve host names.</td>
</tr>
<tr>
<td></td>
<td>■ 0 – Do not use IPv6 name services. IPv4 name services are not affected by this setting.</td>
</tr>
<tr>
<td></td>
<td>■ 1 – Use only IPv6 name services. IPv4 name services are disabled by this setting.</td>
</tr>
<tr>
<td></td>
<td>■ 2 – Use IPv6 name services first; use IPv4 name services in case of failure.</td>
</tr>
<tr>
<td></td>
<td>Default value is 2.</td>
</tr>
<tr>
<td>IPv6LinkLocalUnicastScopeId</td>
<td>Specifies an interface name (such as hme0) or index (4) for Solaris/Linux hosts. Specifies an interface index (4) for Windows hosts.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, Steel-Belted Radius does not use link local addresses.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>IPv6SiteLocalUnicastScopeId</td>
<td>Solaris/Linux: Specifies an interface name (such as hme0) or index (4).</td>
</tr>
<tr>
<td></td>
<td>Windows: Specifies an interface index (4).</td>
</tr>
<tr>
<td></td>
<td>If set to 0, Steel-Belted Radius selects the site local scope ID automatically.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
</tbody>
</table>

**[LDAP] Section**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE

**Not used by:** —

The [LDAP] section of radius.ini (Table 17) sets the TCP port number that you want to use for communication between Steel-Belted Radius and LDAP clients.

The syntax is as follows:

```
[LDAP]
Enable = 1
TCPPort = portNumber
```
Table 17: radius.ini [LDAP] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>• If set to 0, the LDAP Configuration Interface is disabled.</td>
</tr>
<tr>
<td></td>
<td>• If set to 1, the LDAP Configuration Interface is enabled.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Enabling LCI without changing the access password might</td>
</tr>
<tr>
<td></td>
<td>leave your Steel-Belted Radius database vulnerable to access by any</td>
</tr>
<tr>
<td></td>
<td>LDAP client. Read the “LDAP Configuration Interface” chapter of the</td>
</tr>
<tr>
<td></td>
<td>Steel-Belted Radius Administration Guide before you enable this feature.</td>
</tr>
<tr>
<td>TCPPort</td>
<td>Specifies the TCP port number that you want to use for communication</td>
</tr>
<tr>
<td></td>
<td>between Steel-Belted Radius and LDAP clients.</td>
</tr>
<tr>
<td></td>
<td>Default value is 667.</td>
</tr>
</tbody>
</table>

**[LDAPAddresses] Section**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

The [LDAPAddresses] section of radius.ini lets you specify the interfaces on which Steel-Belted Radius listens for LDAP Configuration Interface (LCI) requests. If you want to provide these settings, you must add a section called [LDAPAddresses] to the radius.ini file. This section should contain a list of IP addresses, one per line:

```
[LDAPAddresses]
199.198.197.196
196.197.198.199
```

If the [LDAPAddresses] section is omitted or empty, Steel-Belted Radius listens for LCI requests on all bound IP interfaces.

**EE:** The LDAP Configuration Interface is an optional add-on for the Enterprise edition of Steel-Belted Radius. You must license the LDAP Configuration Interface before you can configure or use it.

**[MsChapNameStripping] Section**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not used by:** —

The [MsChapNameStripping] section of radius.ini (Table 18) specifies whether you want Steel-Belted Radius to try to strip domain information from usernames when it tries to match its user entry to the username/password hash forwarded by the enduser. This feature is useful in situations where the username in the Steel-Belted Radius database includes characters the enduser host considers domain information, which it deletes before computing its hash of the user’s credentials.
If this feature is enabled:

1. Steel-Belted Radius scans the username in its database looking for delimiter characters that might indicate a domain is prefixed to the username. If a prefix delimiter character is found, the server strips that character (and all characters to the left of the delimiter), generates its own hash of the user’s credentials, and compares the result to the hashed credentials forwarded by the enduser to determine if a match is found.

2. If a prefix delimiter is not found (or if the hashed credentials do not match after the prefix is stripped), Steel-Belted Radius scans the username looking for delimiter characters that might indicate a domain is suffixed to the username. If a suffix delimiter character is found, the server strips that character (and all characters to the right of the delimiter), generates its own hash of the user’s credentials, and compares the result to the hashed credentials forwarded by the enduser to determine if a match is found.

3. If neither a prefix delimiter nor a suffix delimiter is found (or if a delimiter was found but the hashed credentials did not match), the server uses the entire username string to generate the hashed credentials and compares the result to the hashed credentials forwarded by the enduser to determine if a match is found.

The syntax for the [MsChapNameStripping] section is as follows:

```ini
[MsChapNameStripping]
Enable=1
Prefix=\\
Suffix=@/
```

Table 18: radius.ini [MsChapNameStripping] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | - If set to 0 (or omitted), MS-CHAP name stripping is disabled.  
- If set to 1, MS-CHAP name stripping is enabled.  
Default value is 0. |
| Prefix    | A list of as many as five ASCII characters to strip from the prefix.  
If a space character appears in the list, the entire list must be surrounded by quotation marks.  
Enter a double backslash (\\) to indicate you want to strip the backslash character. A double backslash counts as one character in the list.  
Default value is \\ |
| Suffix    | A list of as many as five ASCII characters to strip from the suffix.  
If a space character appears in the list, the entire list must be surrounded by quotation marks.  
Enter a double backslash (\\) to indicate you want to strip the backslash character. A double backslash counts as one character in the list.  
Default value is /@ |
[Ports] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE
Not used by: —

The [Ports] section of `radius.ini` (Table 19) provides a method for setting the UDP ports used by Steel-Belted Radius.

- If one or more UDPAuthPort settings are specified in the [Ports] section of `radius.ini`, the port numbers in this section are the only ones on which the server listens for authentication requests. Similarly, if one or more UDPAcctPort settings are specified, they are the only ones on which the server listens for accounting requests.

You can specify as many as 64 port numbers on a Windows server and as many as 4096 ports on a Solaris or Linux server. If this limit is exceeded, the RADIUS authentication subcomponent fails to initialize.

- If no UDPAuthPort or UDPAcctPort settings are present in the [Ports] section, the server attempts to read the port numbers associated with `radius` service (authentication) and `radacct` (accounting) in `/etc/services`. If successful, the server listens on these port numbers. No more than one port can be specified for the `radius` service or for the `radacct` service.

- If no UDPAuthPort settings are present in the [Ports] section and no `radius` service or `radacct` is listed in the `/etc/services` file, the server listens for authentication requests on UDP ports 1645 and 1812 for authentication and UDP ports 1646 and 1813 for accounting.

NOTE: Any failure to bind to one of the selected UDP ports causes the affected subcomponent (authentication or accounting) to fail to initialize.

If the server will function as a proxy forwarding server, you can specify a block of UDP port numbers from which the proxy RADIUS ports are allocated. Proxy RADIUS allocates port numbers in sets of eight. Port numbers in an allocated block do not have to be contiguous: if a UDP port number that falls in the proxy RADIUS range is in use, proxy RADIUS skips over it.

Table 19: `radius.ini` [Ports] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureTcpAdminAddress</td>
<td>Specifies the IP address of the administrative interface used for communication between SBR Administrator and the Steel-Belted Radius server. If not specified, any network interface on the Steel-Belted Radius server accepts a connection from SBR Administrator.</td>
</tr>
<tr>
<td>SecureTcpAdminPort</td>
<td>Specifies the TCP port used for communication between SBR Administrator and the Steel-Belted Radius server. Default value is 1813.</td>
</tr>
</tbody>
</table>
Chapter 2: Operations Files

For example:

```
[Ports]
SecureTcpAdminPort = 1813
SecureTcpAdminAddress = 192.168.12.15
TcpControlPort = 1812
TCPControlAddress = 192.168.15.55
UDPAuthPort = 1645
UDPAuthPort = 1812
UDPAcctPort = 1646
UDPAcctPort = 1813
UDPPortBlockStart = 28000
UDPPortBlockLength = 64
```

The UDP port assignments entered in the [Ports] section of the `radius.ini` file override the UDP port assignments specified in the `/etc/services` file. For more information, see “services File” on page 53.
**[SecurID] Section**

*Used by:* GEE, SPE, SPE + MIM, SPE + EAP, EE  
*Not used by:* —

The [SecurID] section of radius.ini (Table 20) contains items specific to RSA SecurID authentication for ISDN users. It provides information that allows Steel-Belted Radius to cache the user’s credentials temporarily after a successful SecurID authentication. This technique is necessary to permit a second ISDN B-channel to be authenticated during the user’s session. Steel-Belted Radius uses the cached token to authenticate the second channel.

**NOTE:** If this feature is not enabled, users who want to authenticate against a SecurID database through an ISDN connection that “bonds” both B-channels will fail to authenticate due to a SecurID security violation. ISDN users running only one B-channel are not affected.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| CachePasscodes          | ■ If set to yes, RSA SecurID passcode caching is enabled.  
|                         | ■ If set to no, RSA SecurID passcode caching is disabled.  
|                         | Default value is no.                                                    |
| SecondsToCachePasscodes | The number of seconds to retain the cached SecurID passcode (PIN and token code).  
|                         | Default value is 60 seconds.                                             |

**[Self] Section**

*Used by:* GEE, SPE, SPE + MIM, SPE + EAP  
*Not used by:* EE

The [Self] section of radius.ini lists all the realm names that indicate this Steel-Belted Radius server should handle a request. The syntax is as follows:

```
[Self]
RealmName
RealmName

; 
```

You can use the [Self] section to map a realm name to the Steel-Belted Radius server. If you acquire a batch of new user accounts, users do not have to change how they enter usernames. They can enter the name `User<Delimiter>RealmName` or `RealmName<Delimiter>User` as usual.

When a username comes into Steel-Belted Radius, if the [Self] section lists `RealmName`, Steel-Belted Radius understands that it is the target, and handles the request locally instead of directing the request elsewhere.
**[StaticAcctProxy] Section**

The [StaticAcctProxy] section of radius.ini controls the delivery of Accounting messages to additional RADIUS accounting-enabled devices on the network, even when the initial RADIUS transaction is not a proxy RADIUS transaction. The syntax is as follows:

```
[StaticAcctProxy]
target = proxy
```

where `proxy` identifies the name of the RADIUS accounting-enabled device.

**[Strip] Section**

*Used by:* GEE, SPE, SPE + MIM, SPE + EAP,  
*Not used by:* EE

The [Strip] section specifies how Steel-Belted Radius manipulates the username by stripping the incoming `User-Name` attribute value of realm names and other “decorations.”

The [Strip] section (and accompanying [StripPrefix] and [StripSuffix] sections) look like the following:

```
[Strip]
Authentication=Yes
Accounting=No
StripPrefixCharacters=@#%
StripSuffixCharacters="! 
```

```
[StripPrefix]
PrefixStringToStrip1
PrefixStringToStrip2
```

```
[StripSuffix]
SuffixStringToStrip1
SuffixStringToStrip2
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>If set to yes, the [StripPrefix] and [StripSuffix] rules are used to strip the username before an authentication request is processed. Default value is no.</td>
</tr>
<tr>
<td>Accounting</td>
<td>If set to yes, the [StripPrefix] and [StripSuffix] rules are used to strip the username before an accounting request is processed. Default value is no.</td>
</tr>
<tr>
<td>StripPrefixCharacters</td>
<td>A list of ASCII characters to strip from the prefix. If a space character appears in the list, the entire list must be surrounded by quotation marks.</td>
</tr>
<tr>
<td>StripSuffixCharacters</td>
<td>A list of ASCII characters to strip from the suffix. If a space character appears in the list, the entire list must be surrounded by quotation marks.</td>
</tr>
</tbody>
</table>
[StripPrefix] Section

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP
**Not used by:** EE

The [StripPrefix] section lists prefixes that should be removed from the beginning of usernames, including the delimiter. If a space character appears in the list, the entire list must be surrounded by quotation marks.

```
[Strip]
  Authentication=yes
  Accounting=yes

StripPrefix
  isp.com\n  att.net]
```

In this example, Steel-Belted Radius would strip the prefixes `isp.com\` and `att.net` from usernames in authentication and accounting requests.

[StripSuffix] Section

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP
**Not used by:** EE

The [StripSuffix] section lists suffixes that should be removed from the end of usernames, including the delimiter.

For example:

```
[Strip]
  Authentication=yes
  Accounting=yes

StripSuffix
  @myrealm.com
  @yahoo.com
```

In this example, Steel-Belted Radius would strip the suffixes `@myrealm.com` and `@yahoo.com` from usernames in authentication and accounting requests.

[UserNameTransform] Section

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE
**Not Used By:** —

The [UserNameTransform] section (Table 22) lets you specify a rule for transforming user names in RADIUS requests from the form in which they are received to a form in which they can be processed. This can be useful when the form in which users supply their names to the network access device is not compatible with the form in which the RADIUS server applies its rules for proxy forwarding or with the form that the authentication system requires.
The user name transformation rule used to convert input strings to output strings is based on an input format and an output format. The user name transformation rule is applied to user names appearing in RADIUS requests. The user name from the RADIUS request is parsed based on the input format.

- If the user name does not conform to the input format, the rule does not apply and the user name is unchanged.

- If the rule does apply, the parsed elements of the user name are formatted based on the output format to construct the transformed user name:

  1. The User-Name from the Access-Accept (or Acct-Start/Acct-Stop) is compared to the input format rule.

  2. If the User-Name matches the rule, it is modified into the output format, and authentication continues.

  3. If the User-Name does not match the input format, no modification occurs, and authentication continues.

The transformed user name replaces the original user name in RADIUS processing, just as if the transformed user name had been included in the request. The decision to proxy-forward the packet is based on the transformed user name, and all authentications are based on the transformed user name.

Format strings can be any sequence of characters, and can contain embedded variables enclosed in angle brackets (< >). The backslash (\) is an escape character within text, used to represent literal characters. Within variable names, a backslash is treated as a character, not as an escape; and therefore, variable names may not include right angle brackets (>).

The literal text should be composed of characters not expected to be found in the variable elements. Use punctuation characters such as a slash (/) or an at-sign (@), rather than letters or numbers.

The user name transformation rule can be applied to authentication packets, accounting packets, or both.

```ini
[UserNameTransform]
In=<input format>
Out=<output format>
Accounting=<yes | no>
Authentication=<yes | no>
```

Table 22: radius.ini [UserNameTransform] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>In</td>
<td>A format string identifying the input format for user names. For example, <code>&lt;user&gt; @ &lt;realm&gt;</code></td>
</tr>
<tr>
<td>Out</td>
<td>A format string identifying the output format for user names. For example, <code>&lt;user&gt;</code></td>
</tr>
<tr>
<td>Authentication</td>
<td>Set to Yes to enable the transform for authentication requests. Default value is Yes.</td>
</tr>
</tbody>
</table>
For example, the following settings transforms `george@acme.com` to `george`:

```
In = <user>@<realm>
Out = <user>
```

The following settings transform `abc/martha@bigco.com` to `bigco.com::abc/martha`:

```
In = <prefix>/<user>@<realm>
Out = <realm>::<prefix>/user
```

### [ValidateAuth] and [ValidateAcct] Sections

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

The [ValidateAuth] and [ValidateAcct] sections of `radius.ini` (Table 23) specify how Steel-Belted Radius validates usernames in authentication and accounting requests. These sections enable Steel-Belted Radius to examine the User-Name attribute in the incoming packet to determine whether it employs a valid character set.

```
[ValidateAuth]
User-Name = RegularExpression

[ValidateAcct]
User-Name = RegularExpression
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ValidateAuth]</td>
<td>This section applies only to authentication servers.</td>
</tr>
<tr>
<td>[ValidateAcct]</td>
<td>This section applies only to accounting servers.</td>
</tr>
<tr>
<td>User-Name</td>
<td>Names the regular expression against which the User-Name attribute is validated. If the User-Name entry is absent from the section or the regular expression is blank, no validation occurs.</td>
</tr>
</tbody>
</table>
Table 23: radius.ini [ValidateAuth] and [ValidateAcct] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RegularExpression</td>
<td>The regular expression lists each valid character or range of characters.</td>
</tr>
<tr>
<td></td>
<td>A dash (-) indicates a range of alphanumeric characters. For example, A-Z</td>
</tr>
<tr>
<td></td>
<td>indicates every uppercase alphabetic character.</td>
</tr>
<tr>
<td></td>
<td>A backslash () followed by a non-alphanumeric character indicates that</td>
</tr>
<tr>
<td></td>
<td>character literally, for example ? indicates the question mark.</td>
</tr>
<tr>
<td></td>
<td>\ is used as an escape character, as follows:</td>
</tr>
<tr>
<td></td>
<td>\a: bell (7)</td>
</tr>
<tr>
<td></td>
<td>\b: backspace (8)</td>
</tr>
<tr>
<td></td>
<td>\t: tab (0x09)</td>
</tr>
<tr>
<td></td>
<td>\n: newline (10)</td>
</tr>
<tr>
<td></td>
<td>\w: vertical tab (11)</td>
</tr>
<tr>
<td></td>
<td>\f: formfeed (12)</td>
</tr>
<tr>
<td></td>
<td>\r: return (13)</td>
</tr>
<tr>
<td></td>
<td>\xmn: hex value, where mn is a two-digit hexadecimal number</td>
</tr>
<tr>
<td></td>
<td>\nnn: decimal value, where nnn is a three-digit decimal number</td>
</tr>
</tbody>
</table>

The following example permits a string composed only of upper-case and lower-case characters, digits, periods, and commas:

    User-Name = A-Za-z0-9.,

The following example permits upper-case and lower-case characters:

    User-Name = A-Za-z
sbrd.conf File (Solaris/Linux only)

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The sbrd.conf file (Table 24) is an executable Bourne shell script that is invoked by the sbrd process to initialize the execution environment for Steel-Belted Radius.

**NOTE:** In Steel-Belted Radius v5.3, users were instructed to modify the sbrd script if they wanted to change its settings. The sbrd.conf file makes direct modification to the sbrd script unnecessary. Do not modify the sbrd script.

For example:

```bash
#!/bin/sh
##############
# sbrd.conf
##############
ULIMIT_CORE_SIZE=""
ULIMIT_CORE_COUNT=3
ULIMIT_OPEN_FILES=1024
RADIUSUMASK=""
RADIUS_HIGH_FDS=1
ORACLE_MSB_FILE="ORACLE_HOME/rdbms/mesg/ocius.msb"

# Radius executable, options, and arguments
RADIUS="radius"
RADIUSOPTS=""
RADIUSARGS="sbr.xml"
RADIUS_PRIVATE_DIR="$RADIUSDIR"

# Watchdog executable, options, and arguments
WATCHDOGENABLE=0
WATCHDOG="radiusd"
WATCHDOGOPTS="--config $RADIUSDIR/radiusd.conf --pidfile $RADIUSDIR/radius.pid"
WATCHDOGARGS="$RADIUSDIR/$SELF"
```

**NOTE:** Do not include spaces in parameter settings in the sbrd.conf file.

**Correct:** ULIMIT_CORE_COUNT=3  
**Incorrect:** ULIMIT_CORE_COUNT = 3
Table 24: sbrd.conf Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ULIMIT_CORE_SIZE</td>
<td>Specifies the size of core files generated if Steel-Belted Radius fails. If set to a value, ULIMIT_CORE_SIZE specifies the maximum size for core files in 512-byte blocks (Solaris) or in 1024-byte blocks (Linux). If set to disabled, Steel-Belted Radius uses the current environment without changes. If set to &quot;&quot; (two double-quotes with no space between), Steel-Belted Radius uses the current environment, making adjustments as needed. Default value is &quot;&quot;.</td>
</tr>
<tr>
<td>ULIMIT_CORE_COUNT</td>
<td>Specifies the number of core files maintained on the Steel-Belted Radius server. If the maximum number of core files already exists on the server, Steel-Belted Radius discards the oldest core files and generates a new core file if it fails. If set to a number in the range 0–999,999,999, the server maintains the specified number of core files. If set to unlimited, Steel-Belted Radius does not discard existing core files if it generates a new one. If set to disabled, Steel-Belted Radius uses the current environment without changes. If set to &quot;&quot; (two double-quotes with no space between), Steel-Belted Radius uses the current environment, making adjustments as needed. Default value is 3.</td>
</tr>
<tr>
<td>ULIMIT_OPEN_FILES</td>
<td>Specifies the number of open files that the Steel-Belted Radius process can have open at one time. If set to a number in the range 256–1024, the server maintains the specified number of open files. If set to disabled, Steel-Belted Radius uses the current environment without changes. If set to &quot;&quot; (two double-quotes with no space between), Steel-Belted Radius uses the current environment, making adjustments as needed. Default value is 1024.</td>
</tr>
<tr>
<td>RADIUSSMASK</td>
<td>Specifies the file permissions that are withheld when new log files are created. If set to a umask argument, log files are created with the specified permissions withheld from Owner, Group, and Other users. If set to &quot;&quot;, log files are created with the default access permissions established by the ambient umask for Owner, Group, and Other users. Refer to the Steel-Belted Radius Administration Guide for information on how to configure and use umask to control file permission settings.</td>
</tr>
</tbody>
</table>
Table 24: sbrd.conf Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| RADIUS_HIGH_FDS      | ■ If set to 0, management of file descriptors is disabled. You can set RADIUS_HIGH_FDS to 0 if you specified a value of 256 or lower for the ULIMIT_OPEN_FILES parameter.  
  ■ If set to 1, management of file descriptors is enabled. You should set RADIUS_HIGH_FDS to 1 if you specified a value greater than 256 for the ULIMIT_OPEN_FILES parameter.  
  Default value is 1.                                                                 |
| ORACLE_MSB_FILE      | Specifies the absolute path to the locale-specific Oracle message file.  
  ■ If you enter the path name to a message file, the file descriptor that is returned is greater than 255.  
  ■ If you enter "", Steel-Belted Radius uses the descriptor returned by a standard library open() call. |
| RADIUS               | Default value is “radius”.  
  Do not change this value unless instructed to do so by technical support.                                                          |
| RADIUSOPTS           | Specifies options used when running Steel-Belted Radius.  
  Default value is "".  
  Do not change this value unless instructed to do so by technical support.                                                              |
| RADIUSARGS           | Default value is “sbr.xml”.  
  Do not change this value unless instructed to do so by technical support.                                                              |
| RADIUS_PRIVATE_DIR   | Default value is “$RADIUSDIR”.  
  Do not change this value unless instructed to do so by technical support.                                                              |
| WATCHDOGENABLE       | ■ If set to 0, the Steel-Belted Radius watchdog process, which restarts Steel-Belted Radius if it fails, is disabled.  
  ■ If set to 1, the Steel-Belted Radius watchdog is enabled.  
  Default value is 0.                                                                                                                  |
| WATCHDOG             | Specifies the name of the Steel-Belted Radius watchdog process.  
  Default value is radiusd.  
  Do not change this value unless instructed to do so by technical support.                                                              |
| WATCHDOGOPTS         | Default value is -config $RADIUSDIR/radiusd.conf --pidfile $RADIUSDIR/radiusd.pid.  
  Do not change this value unless instructed to do so by technical support.                                                              |
| WATCHDOGARGS         | Default value is $RADIUSDIR/$SELF.  
  Do not change this value unless instructed to do so by technical support.                                                              |
services File

The services file can be used to assign default UDP ports for RADIUS communications to and from the Steel-Belted Radius server. Steel-Belted Radius reads the services file at startup. Among the items of information in the services file are the port assignments for RADIUS authentication and accounting services.

Figure 1 illustrates part of a sample services file.

**Figure 1: Sample Services File**

```
# This file contains port numbers for well-known services
# defined by IANA. Format:
#
# <service> <port number>/<protocol> [aliases...] [#<comment>]
#
  echo    7/tcp
  echo    7/udp
  discard 9/tcp  sink null
  discard 9/udp  sink null
  systat  11/tcp users #Active users
  systat  11/tcp users #Active users
  daytime 13/tcp
```

The location of the services file depends on your operating system:

- **Solaris/Linux**: `/etc/` (may be mapped using NIS or NIS+)
- **Windows**: `C:\WINDOWS\system32\drivers\etc\`

If no entry for radius or radacct is found in the services file, Steel-Belted Radius uses the default UDP ports (1645 and 1812 for authentication, 1646 and 1813 for accounting).

Steel-Belted Radius can be configured to use any available UDP ports for authentication and accounting:

1. Use a text editor to open the services file.

2. To set the port for authentication, set the value of the radius parameter. For example:

   `radius 1812/udp # RADIUS authentication protocol`

3. To set the port for accounting, set the value of the radacct parameter. For example:

   `radacct 1813/udp # RADIUS accounting protocol`

**NOTE:** Port number assignments made in the radius.ini file override the assignments made in this file. See “[Ports] Section” on page 42 for more information.
You can determine the ports that Steel-Belted Radius is using at any time by examining the server log file for that time period.

**NOTE:** If another RADIUS server is running on the same host, you must modify the services file to avoid port number conflicts if the other RADIUS server binds to the default ports before Steel-Belted Radius starts.
servtype.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP

**Not used by:** EE

The servtype.ini file configures service type mapping in Steel-Belted Radius. Service type mapping allows a single user to have multiple authorization attribute sets based on the service type the user is requesting. The service type is determined based on request attributes using rules that may differ depending on the network access device.

Using static configuration parameters in the servtype.ini file, you can specify, on a device-by-device basis, a mapping of request attributes and/or values to service type strings. These strings can be attached to the username as a prefix or as a suffix. The elaborated username is used for both authentication and authorization, and for allowing different authorizations based on service type requested.

Refer to the *Steel-Belted Radius Administration Guide* for information on how to configure and use service type mapping.

**[Settings] Section**

The [Settings] section of servtype.ini (Table 25) controls how the service type string should be attached to the username prior to look-up in the Native User database.

---

**NOTE:** If Prefix and Suffix are both set to 0 in the [Settings] section, service type mapping is disabled.

---

**Table 25: servtype.ini [Settings] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Prefix    | Specifies whether the service type string should be prefixed to the username prior to look-up in the Native User database.  
  - If set to 1, the service type string is prefixed to the username.  
  - If set to 0, the service type string is not prefixed to the username.  
  Default value is 0. |
| Suffix    | Specifies whether the service type string should be suffixed to the username prior to look-up in the Native User database.  
  - If set to 1, the service type string is suffixed to the username.  
  - If set to 0, the service type string is not suffixed to the username.  
  Default value is 0. |
| Default   | Mapping name that is used when an Access-Request message is received from a network access device not listed in the [NAS] section of servtype.ini.  
  If you do not configure a Default setting and the server cannot determine the mapping in any other way, the server ignores the service type and authenticates the user without it. |
[NAS] Section

The [NAS] section of the servtype.ini file lets you map network access devices to [mapping] sections. The syntax for [NAS] is as follows:

```
[NAS]
NASname = mappingName
NASname = mappingName
```

Each NASname entry in the [NAS] section must match the name of a RADIUS client entry in the Steel-Belted Radius database. When an Access-Request is received, its NAS-IP-Address attribute is matched to a RADIUS client entry in the database. If a match can be found and the RADIUS client name matches a NASname in the [NAS] section, Steel-Belted Radius looks for a corresponding [Mapping] section in the servtype.ini file.

[MappingName] Section

Each [MappingName] section of the servtype.ini file identifies the strings to be added to the username for lookups in the Native User database, which allows Steel-Belted Radius to retrieve the appropriate return list, and specifies the rules an incoming Access-Request packet must meet before Steel-Belted Radius returns an Access-Accept message. The name of each [MappingName] section must match a mappingName entry in the [NAS] section.

The syntax for each [MappingName] section is as follows:

```
[mapping]
ServiceTypeString
   RADIUSattribute = value
   ~RADIUSattribute = value
```

Each rule is a statement about an attribute that must be present in the incoming Access-Request packet. Each rule must be indented with a tab character, followed by a RADIUSattribute = value string, followed by a carriage return. Every component of the rule is optional, so there are many syntax variations.

If a rule includes a RADIUSattribute field, this field must identify a standard or vendor-specific RADIUS attribute that is known to the server. If a rule provides an optional value field, this field must name a valid possible value for that attribute.

If the RADIUSattribute field for a rule is preceded by a tilde (~), then the specified RADIUSattribute, if present in the Access-Request packet, must have a value other than value for the rule to be true. If the RADIUSattribute is not present in the Access-Request packet, or if it is present and has the value specified, the rule is false and authorization fails.

Example

```
[Settings]
Prefix=1
Suffix=0
Default=defaultmap

[NAS]
nas1=nas1map
```
nas2=nas2map

[nas1map]
ppp:
   Framed-Protocol=1
   Service-Type=2
vpn:
   Framed-Protocol=6
   ~Service-Type=2
other:
   Framed-Protocol
   Service-Type

[nas2map]
analog:
   NAS-Port-Type=1
isdn:
   NAS-Port-Type=2
[defaultmap]
ppp:
update.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

The `update.ini` initialization file controls what information is updated when Steel-Belted Radius receives a HUP or USR2 signal, which is sent by means of the `signal` command on Solaris and Linux and by means of the `radhup.exe` and `radusr2.exe` programs on Windows.

When Steel-Belted Radius receives a HUP or USR2 signal, it performs the tasks specified in the [HUP] and [USR2] sections of the `update.ini` file. You can perform tasks selectively by modifying `update.ini` to toggle specific settings; for example, you can issue a HUP signal to initiate one set of tasks, and then modify `update.ini` and issue another HUP signal to initiate a different set of tasks.

The `update.ini` file installed with Steel-Belted Radius causes Steel-Belted Radius to re-read all settings when it receives a HUP signal and to clear its statistics when it receives a USR2 signal.

**[HUP] and [USR2] Sections**

The [HUP] section of `update.ini` specifies what tasks Steel-Belted Radius should perform when it receives a HUP signal. The [USR2] section of `update.ini` specifies what tasks Steel-Belted Radius should perform when it receives a USR2 signal.

```ini
[HUP]
ResetStats = 0
ResetThreadHighWaterMarks = 0
Update3GPP = 1
Update3GPP2 = 1
UpdateAdminAccess = 1
UpdateAutoStop = 1
UpdateCCAGateways = 1
UpdateDHCPPools = 1
UpdateEap = 1
UpdateLogAndTraceLevel = 1
UpdateLogfilePermissions = 1
UpdatePlugins = 1
UpdateProxy = 1
UpdateValuePools = 1
```

Table 26 lists the settings that may be present in the [HUP] or [USR2] section of `update.ini`. 

---

58  update.ini File
# Table 26: update.ini Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| ResetStats              | - If set to 0, do not reset Steel-Belted Radius statistics to 0 when a HUP or USR2 signal is received.  
                          | - If set to 1, reset Steel-Belted Radius statistics to 0 when a HUP or USR2 signal is received.  
                          | Default value is 0 in the [HUP] section.  
                          | Default value is 1 in the [USR2] section. |
| ResetThreadHighWaterMarks | - If set to 0, do not reset Steel-Belted Radius high thread statistics (High-Auth-Threads-Since-Reset,  
                             | High-Acct-Threads-Since-Reset, and  
                             | High-Total-Threads-Since-Reset) when a HUP or USR2 signal is received.  
                          | - If set to 1, reset Steel-Belted Radius high thread statistics to 0 when a HUP or USR2 signal is received.  
                          | Default value is 0 in the [HUP] section.  
                          | Default value is 1 in the [USR2] section. |
| Update3GPP              | - If set to 0, do not update 3GPP settings from 3gpp.ini when a HUP or USR2 signal is received.  
                          | - If set to 1, update 3GPP settings from 3gpp.ini when a HUP or USR2 signal is received.  
                          | Default value is 1 in the [HUP] section.  
                          | Default value is 0 in the [USR2] section. |
| UpdateAutoStop          | - If set to 0, do not update the Proxy AutoStop settings (by re-reading the AcctAutoStopEnable setting in radius.ini) when a HUP or USR2 signal is received.  
                          | - If set to 1, update the Proxy AutoStop settings (by re-reading the AcctAutoStopEnable setting in radius.ini) when a HUP or USR2 signal is received.  
                          | Default value is 1 in the [HUP] section.  
                          | Default value is 0 in the [USR2] section. |
### Table 26: update.ini Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpdateCCAGateways</td>
<td>If set to 0, do not update 3Com CCA gateways (specified in ccagw.ini) when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, update 3Com CCA gateways (specified in ccagw.ini) when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 in the [HUP] section.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 in the [USR2] section.</td>
</tr>
<tr>
<td>UpdateDHCPPools</td>
<td>If set to 0, do not update DHCP pool settings specified in dhcp.ini when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, update DHCP pool settings specified in dhcp.ini when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 in the [HUP] section.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 in the [USR2] section.</td>
</tr>
<tr>
<td>UpdateEAP</td>
<td>If set to 0, do not update EAP settings specified in eap.ini when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, update EAP settings specified in eap.ini when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 in the [HUP] section.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 in the [USR2] section.</td>
</tr>
<tr>
<td>UpdateLogAndTraceLevel</td>
<td>If set to 0, do not update log and trace levels specified in radius.ini when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, update log and trace levels specified in radius.ini when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 in the [HUP] section.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 in the [USR2] section.</td>
</tr>
<tr>
<td>UpdateLogfilePermissions</td>
<td>If set to 0, do not update logfile permissions specified in the logfile configuration files when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td>(Solaris/Linux only)</td>
<td>If set to 1, update logfile permissions specified in the logfile configuration files when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 in the [HUP] section.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 in the [USR2] section.</td>
</tr>
<tr>
<td>UpdatePlugins</td>
<td>If set to 0, do not update plug-ins that support dynamic re-reading of configuration settings when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, update plug-ins that support dynamic re-reading of configuration settings when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 in the [HUP] section.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 in the [USR2] section.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The TLS, TTLS, and PEAP plug-ins currently support dynamic configuration updates.</td>
</tr>
<tr>
<td>UpdateProxy</td>
<td>If set to 0, do not update realm configuration when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, update realm configuration (by re-reading proxy.ini, *.pro, and *.dir files) when a HUP or USR2 signal is received.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 in the [HUP] section.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 in the [USR2] section.</td>
</tr>
</tbody>
</table>
**Table 26: update.ini Syntax (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| UpdateValuePools   | - If set to 0, do not update attribute value pool settings (in *.rr files when a HUP or USR2 signal is received.  
                      - If set to 1, update attribute value pool settings (in *.rr files when a HUP or USR2 signal is received).  
                      Default value is 1 in the [HUP] section.  
                      Default value is 0 in the [USR2] section. |
Auto-Restart Files (Solaris/Linux only)

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

When enabled, the auto-restart module acts as a watchdog daemon, monitoring the status of the Steel-Belted Radius executable and restarting it as needed. Automatic restart is disabled by default.

Perl must be installed on the Steel-Belted Radius server if you want the automatic restart module. Perl support is not required for syslog but is available.

**Perl SNMP Support**

You can configure the auto-restart module to send SNMP traps to record auto-restart events. Perl SNMP support resides in the Perl SNMP_Session module, which provides access to remote SNMP agents. Refer to the ReleaseNotes.txt file for radiusd for information on how to install and configure the Perl SNMP_Session module.

Perl SNMP support allows Steel-Belted Radius to send SNMP traps to a variety of SNMP agents, including the Sun Management Center, which is distributed with some Sun hardware platforms. Sun Management Center is not required to run radiusd.

**Perl syslog Support**

The optional perl package syslog.ph is used to log the watchdog daemon status. You can configure the auto-restart module to send syslog messages to record auto-restart events. To use syslog reporting, you can use the h2ph utility to create a syslog.ph file. The following example assumes site_perl/5.005 is in @INC:

```
su - root  
cd /user/include/sys  
/usr/perl15/bin/h2ph -d /usr/perl15/site_perl/5.005 syslog.h
```

If you do not want to use syslog, you should use the -d or --logfile options for the radiusd command to open a regular log file (radiusd.log).

**S90radius/sbrd Script**

To enable the auto-restart module, you must edit the S90radius script (Solaris) or sbrd script (Linux) to ensure that a certain line in the script is uncommented (the hash mark # is removed from the start of the line), as follows:

1. If Steel-Belted Radius is already running, become superuser and type the following command to stop the server:

   **Solaris:** /etc/rc2.d/S90radius stop  
   **Linux:** /etc/init.d/sbrd stop
2. Edit the `radius` script (`S90radius` or `sbrd`). The line you want to edit for auto-restart appears as follows:

```
# RADIUS="$RADIUSDIR/radiusd --server $RADIUSDIR/radius"
```

The `-server` option identifies the location and name of the Steel-Belted Radius executable file, and must be present on the `radiusd` command line.

3. If the comment hash mark `#` is present at the start of the line, remove it.

4. Save and exit the file.

5. Type the following command to restart the server: `S90radius` or `sbrd` invokes `radiusd`, which starts the RADIUS service:

```
Solaris: /etc/rc2.d/S90radius start
Linux: /etc/init.d/sbrd start
```

### `radiusd` Script

If you enable the auto-restart module, the `S90radius/sbrd` startup/shutdown script runs `radiusd` instead of the `radius` executable file. `radiusd` executes `radius` as a child process and monitors its health by a polling mechanism. Polling parameters are configurable by editing the `radiusd.conf` file in the server directory; the relevant timeouts and logging options are near the beginning of the file.

The default `radiusd.conf` settings cause the auto-restart feature to work as follows:

If the `radius` server executable fails to respond to status polling from `radiusd` within 17 seconds, `radiusd` attempts to stop `radius` using `SIGTERM` (a polite shutdown). If `radius` does not shut down within 60 seconds, `SIGKILL` (a hard kill) is used to stop it. After shutdown by either method, `radiusd` starts a new `radius` child process. If this `radius` child does not respond to status polling within 60 seconds of startup, it is presumed dead; a misconfiguration of the server is assumed; and `radiusd` terminates with a critical error.

---

**NOTE:** The `radius` executable normally runs as a daemon. When the automatic-restart module is enabled, the `radius` executable is run as a child process of `radiusd` instead of being run as a daemon.

While the auto-restart module is enabled, all informational, debugging, warning, error, and critical messages from `radiusd` are recorded in the following locations:

- **Syslog** – Messages are written to the `syslog` system logging facility.

- **Log file** – If `syslog` is not available, messages are written to the server log file specified using the `-logfile` option on the `radiusd` command line; for example:

```
RADIUS="$RADIUSDIR/radiusd \ 
-server $RADIUSDIR/radius \ 
-logfile /var/log/radd.log"
```
If the \texttt{-logfile} option is not already included in the \texttt{radiusd} command line, you may add it.

\begin{table}[h]
\centering
\begin{tabular}{|l|p{0.7\textwidth}|}
\hline
\texttt{radiusd.conf Parameter} & \texttt{Function} \\
\hline
\texttt{WatchdogIntervalPing} & Number of seconds the automatic-restart module waits between sending status inquiries. Default value is 5 seconds. \\
\hline
\texttt{WatchdogIntervalMaxPong} & Number of seconds the automatic-restart module waits for a reply before issuing a \texttt{SIGTERM} (shutdown) message. Default value is 17 seconds. \\
\hline
\texttt{WatchdogIntervalMaxStartup} & Number of seconds during which the server is expected to be able to start up. Default value is 60 seconds. \\
\hline
\texttt{WatchdogIntervalMaxShutdown} & Number of seconds during which the server is expected to be able to shut down. Default value is 60 seconds. \\
\hline
\end{tabular}
\end{table}

\textbf{NOTE:} Options processed by \texttt{radiusd} are preceded by two dashes (\texttt{--}). Options preceded with a single dash are passed to Steel-Belted Radius.

\begin{table}[h]
\centering
\begin{tabular}{|l|}
\hline
\end{tabular}
\end{table}

\textbf{NOTE:} If Perl is not installed in the \texttt{/usr/local/bin/} directory, the following error message occurs when you start the Steel-Belted Radius server:

\begin{verbatim}
./S90radius: /RadiusHome/radiusd: not found
\end{verbatim}

To fix this error, edit the first line of the \texttt{radiusd} file in the RADIUS directory so that the directory structure points to the correct Perl interpreter executable:

\begin{verbatim}
#!/usr/local/bin/perl
\end{verbatim}

\textbf{Script Configuration}\n
The \texttt{radiusd.conf} configuration file (Table 27) provides settings for the \texttt{radiusd} automatic-restart module.
### Table 27: radiusd.conf Syntax  (continued)

<table>
<thead>
<tr>
<th>radiusd.conf Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| **SnmpManager = hostname community port version** | Identifier for an SNMP management station that should receive traps from the automatic-restart module. You can specify more than one SNMP management station. For each SNMP management station, enter the following:  
  - `hostname` – IP address of the SNMP management station.  
  - `community` – SNMP community string.  
  - `port` – UDP port number used for SNMP trap messages. UDP port 162 is the default.  
  - `version` – SNMP version number. Default value is 1.  
If SnmpManager is undefined, SNMP traps may still be logged, but are not transmitted on the network. |
| **SnmpInterface** | Identifies the IP network interface to be used to generate SNMP trap messages. You can specify interfaces by name or by IP address. If you enter any, the first IPv4 interface the automatic-restart module finds is used. If you leave this parameter blank, generation of SNMP trap messages is disabled. |
| **SnmpCommandTrap** | Specifies how SNMP trap messages should be forwarded:  
  - You can specify the pathname and filename for a module or executable whose syntax matches the SMC `snmptrap` utility. For example: `/opt/SUNWsymon/util/bin/sparc-sun-solaris2.8/snmptrap`  
  - You can specify `SNMP_Session.pm` to deliver SNMP traps to the management station using the Perl modules. If you leave the parameter blank, SNMP trap messages are not generated. Default value is blank. |
<p>| <strong>SnmpCommandUptime</strong> | Specifies how the automatic-restart module determines elapsed time for timestamps in trap messages. You can specify the pathname and filename for a module or executable whose syntax matches the SMC <code>uclock</code> utility. For example: <code>/opt/SUNWsymon/util/bin/sparc-sun-solaris2.8/uclock</code> If you leave the parameter blank, the automatic restart module calculates elapsed time relative to its own start time. Default value is blank. |
| <strong>SnmpEnterprise</strong> | Specifies the OID prefix for enterprise-specific trap messages, which is used to select the appropriate MIB for decoding traps. Default value is <code>1.3.6.1.4.1.1411.1.1</code>. If you leave the parameter blank, SNMP trap messages are not generated. |
| <strong>SnmpGenericTrapType = 6</strong> | Specifies the enterprise-specific trap type, which must be 6 according to the SNMPv1 standard. Do not change this value without a specific reason. |</p>
<table>
<thead>
<tr>
<th>radiusd.conf Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnmpTrapWatchdogStarted</td>
<td>Specifies the trap type for messages indicating that the automatic-restart module is started. Default value is 113. Enter 0 to disable this type of trap.</td>
</tr>
<tr>
<td>SnmpTrapWatchdogStopped</td>
<td>Specifies the trap type for messages indicating that the automatic-restart module is stopped. Default value is 114. Enter 0 to disable this type of trap.</td>
</tr>
<tr>
<td>SnmpTrapWatchdogRadiusStarted</td>
<td>Specifies the trap type for messages indicating that the RADIUS server is restarted. Default value is 115. Enter 0 to disable this type of trap.</td>
</tr>
<tr>
<td>SnmpTrapWatchdogRadiusTerm</td>
<td>Specifies the trap type for messages indicating that the RADIUS server is not responding and that the automatic-restart module has sent the SIGTERM signal. Default value is 5028. Enter 0 to disable this type of trap.</td>
</tr>
<tr>
<td>SnmpTrapWatchdogRadiusKill</td>
<td>Specifies the trap type for messages indicating that the RADIUS server is not responding and that the automatic-restart module has sent the KILL signal. Default value is 5029. Enter 0 to disable this type of trap.</td>
</tr>
<tr>
<td>SnmpTrapWatchdogAborted</td>
<td>Specifies the trap type for messages indicating that the RADIUS server is not responding and that the automatic-restart module has given up and aborted. Default value is 10051. Enter 0 to disable this type of trap.</td>
</tr>
<tr>
<td>SnmpTrapWatchdogFailedInit</td>
<td>Specifies the trap type for messages indicating that the automatic-restart module failed to start, which may indicate a misconfiguration issue. Default value is 10052. Enter 0 to disable this type of trap.</td>
</tr>
</tbody>
</table>
Chapter 3

Authentication Configuration Files

This chapter describes the usage and settings for the initialization files used by Steel-Belted Radius to authenticate users and to record the results of authentication events. Initialization files are loaded at startup time, and reside in the Steel-Belted Radius directory.

- authlog.ini File page 68
- authReport.ini File page 73
- authReportAccept.ini File page 75
- authReportBadSharedSecret.ini File page 78
- authReportReject.ini File page 81
- authReportUnknownClient.ini File page 85
- blacklist.ini File page 88
- lockout.ini File page 89
- redirect.ini File page 90
- securid.ini File page 92
- tacplus.ini File page 105
- winauth.aut File page 106
authlog.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP

**Not used by:** EE

The authlog.ini initialization file contains information that controls how RADIUS authentication request attributes are logged in the comma-delimited yyyyymmdd.authlog file.

**[Alias/name] Sections**

You can create one or more [Alias/name] sections in authlog.ini (Table 28) to associate attributes of different names, but identical meaning. For example, one network access device vendor might call an attribute Auth-Connect-Type and another might call it Auth-Conn-Typ, yet the two attributes would both map to Auth-Conn-Type.

Each [Alias/name] section permits you to map one RADIUS authentication request attribute that is already being logged by Steel-Belted Radius to any number of other attributes. You can provide as many [Alias/name] sections as you want, using the following syntax for each section:

```
[Alias/name]
VendorSpecificAttribute=
VendorSpecificAttribute=
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The preferred attribute name. The name attribute must be one that you are currently logging to a column in the Steel-Belted Radius authentication request log file (.authlog). Therefore, it must be listed in the [Attributes] section of authlog.ini.</td>
</tr>
<tr>
<td>VendorSpecificAttribute</td>
<td>Each entry is given on one line. An equal sign (=) must immediately follow each VSA name, without any intervening space. Improperly formatted entries are considered invalid and are ignored.</td>
</tr>
</tbody>
</table>

Each VendorSpecificAttribute in the list is logged to the name column in the authentication request log file. Because you are listing these attributes in an [Alias/name] section, make sure they are not listed in the [Attributes] section or they will be logged to their own columns as well as to the name column.

All of the attribute names that you reference in an [Alias/name] section must be defined in a dictionary file that is already installed on the Steel-Belted Radius server. This includes name and each VendorSpecificAttribute entry.

In the following example, the standard RADIUS attribute Auth-Conn-Type is mapped to the vendor-specific attributes Auth-Connect-Type and Auth-Conn-Typ. Values encountered for all three attributes are logged in the Auth-Octet-Packets column in the authentication request log file:

```
[Alias/Auth-Conn-Type]
VendorSpecificAttribute=
VendorSpecificAttribute=
```
Chapter 3: Authentication Configuration Files

[Attributes] Section

The [Attributes] section of authlog.ini lists all the attributes logged in the authentication request log file. When you install Steel-Belted Radius, the authlog.ini file is set up so that all standard RADIUS attributes and all supported vendor authentication attributes are listed.

You can configure what is logged to the authentication request log file by rearranging the order of attributes in the [Attributes] section. You can delete or comment out attributes you do not want or that do not apply to your equipment. This lets you design the content and column order of any spreadsheets that you plan to create based upon the authentication request log file.

The syntax of the [Attributes] section is as follows:

```
[Attributes]
AttributeName=
AttributeName=
```

For example:

```
[Attributes]
User-Name=
NAS-IP-Address=
NAS-Port=
Service-Type=
Framed-Protocol=
Framed-IP-Address=
Framed-IP-Netmask=
Framed-Compression=
```

The [Attributes] section lists one AttributeName on each line. You must ensure that an equal sign (=) immediately follows each AttributeName, with no spaces in between. Improperly formatted entries are considered invalid and are ignored.

Each AttributeName in the [Attributes] section must be defined in a standard RADIUS or vendor-specific dictionary file (.dct) installed on the Steel-Belted Radius server.

**NOTE:** The first five attributes in each authentication log file entry (Date, Time, RAS-Client, Full-Name, and ACC/REJ) are always enabled, and cannot be re-ordered or deleted. Therefore, these attributes do not appear in the authlog.ini file [Attributes] section.

[Configuration] Section

The [Configuration] section of authlog.ini specifies the location of the yymmdd.authlog file.
Steel-Belted Radius Reference Guide

Table 29: authlog.ini [Configuration] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogDir</td>
<td>Specifies the destination directory on the local host where yyyymmdd.authlog files are stored. Default value is the directory where Steel-Belted Radius is installed. <strong>NOTE:</strong> With directed realms, you can maintain multiple authentication log locations. <strong>NOTE:</strong> You cannot write authlog files to a mapped or shared drive.</td>
</tr>
</tbody>
</table>

[Settings] Section

Steel-Belted Radius writes all authentication request data to the current authentication request log file (yyyymmdd.authlog) until that log file is closed. When Steel-Belted Radius closes an authentication request log file, it immediately opens a new one and begins writing authentication request data to it.

You can configure how often this rollover of the authentication request log file occurs.

The naming conventions of the authentication request log files support the fact that Steel-Belted Radius can create more than one file per day. The formats are as follows. In the examples below, y = year digit, m = month digit, d = day digit, and h = hour digit. The extra sequence number _nnnn starts at _00000 each day.

Table 30: Authentication Log Rollover

<table>
<thead>
<tr>
<th>File Generation Method</th>
<th>File Naming Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default (24 hours)</td>
<td>yyyymmdd.authlog</td>
</tr>
<tr>
<td>Non-24-hour rollover</td>
<td>yyyymmdd_hhmm.authlog</td>
</tr>
<tr>
<td>Rollover due to size</td>
<td>yyyymmdd_nnnnn.authlog</td>
</tr>
<tr>
<td>Rollover due to size or startup when non-24-hour time in effect</td>
<td>yyyymmdd_hhmm_nnnn.authlog</td>
</tr>
</tbody>
</table>

The [Settings] section of authlog.ini (Table 31) controls which entries are written to the authentication request log file, and ensure the compatibility of these entries with a variety of database systems. The following “rollover” settings can be present in the [Settings] section.

Table 31: authlog.ini [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>■ If set to 0, the authentication request log is disabled and other settings are ignored. ■ If set to 1, the authentication request log is enabled. Set Enable to 1 for Authentication servers. For efficiency, set Enable to 0 for non-authentication servers. Default value is 0.</td>
</tr>
</tbody>
</table>
### Chapter 3: Authentication Configuration Files

#### LogFilePermissions
(Solaris/Linux only)

Specifies the owner and access permission setting for the auth log file. Enter a value for the LogFilePermissions setting in *owner:group permissions* format, where:

- **owner** specifies the owner of the file in text or numeric format.
- **group** specifies the group setting for the file in text or numeric format.
- **permissions** specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format.

For example, `ralphw:1007 rw-r-----` specifies that the file owner (ralphw) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and other users cannot access the log file.

#### BufferSize

Specifies the size of the buffer used in the authentication request logging process, in bytes. Default value is 32768.

#### LineSize

Specifies the maximum number of characters in a line in the authentication request log. You can enter a number in the range 1024–32768. Default value is 4096.

#### MaxSize

- If set to a number greater than 0, specifies the maximum number of bytes for an authentication request log file. If the authentication request log file equals or exceeds this limit when the log size is checked, the log file is closed and a new file started.
- If set to 0, the authentication request log has no maximum size. Default value is 0.

**NOTE:** Because the size of the log file is checked once per minute, the log file can exceed the maximum size specified in this parameter.

#### QuoteBinary

- If set to 1, binary values written to the authentication request log file are enclosed in quotes.
- If set to 0, quotes are not used.

Set this value according to the format expected by the application that processes the authentication request log entries. Default value is 1.

#### QuoteInteger

- If set to 1, integer values written to the authentication request log file are enclosed in quotes.
- If set to 0, quotes are not used.

Set this value according to the format expected by the application that processes the authentication request log entries. Default value is 1.

#### QuoteIPAddress

- If set to 1, IP addresses written to the authentication request log file are enclosed in quotes.
- If set to 0, quotes are not used.

Set this value according to the format expected by the application that processes the authentication request log entries. Default value is 1.

---

**Table 31: authlog.ini [Settings] Syntax (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| LogFilePermissions | Specifies the owner and access permission setting for the auth log file. Enter a value for the LogFilePermissions setting in *owner:group permissions* format, where:  
  - **owner** specifies the owner of the file in text or numeric format.  
  - **group** specifies the group setting for the file in text or numeric format.  
  - **permissions** specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format.  
  For example, `ralphw:1007 rw-r-----` specifies that the file owner (ralphw) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and other users cannot access the log file. |
| BufferSize      | Specifies the size of the buffer used in the authentication request logging process, in bytes. Default value is 32768. |
| LineSize        | Specifies the maximum number of characters in a line in the authentication request log. You can enter a number in the range 1024–32768. Default value is 4096. |
| MaxSize         | If set to a number greater than 0, specifies the maximum number of bytes for an authentication request log file. If the authentication request log file equals or exceeds this limit when the log size is checked, the log file is closed and a new file started.  
  - If set to 0, the authentication request log has no maximum size. Default value is 0.  
  **NOTE:** Because the size of the log file is checked once per minute, the log file can exceed the maximum size specified in this parameter. |
| QuoteBinary     | If set to 1, binary values written to the authentication request log file are enclosed in quotes.  
  - If set to 0, quotes are not used.  
  Set this value according to the format expected by the application that processes the authentication request log entries. Default value is 1. |
| QuoteInteger    | If set to 1, integer values written to the authentication request log file are enclosed in quotes.  
  - If set to 0, quotes are not used.  
  Set this value according to the format expected by the application that processes the authentication request log entries. Default value is 1. |
| QuoteIPAddress  | If set to 1, IP addresses written to the authentication request log file are enclosed in quotes.  
  - If set to 0, quotes are not used.  
  Set this value according to the format expected by the application that processes the authentication request log entries. Default value is 1. |
Table 31: authlog.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>QuoteText</td>
<td>■ If set to 1, text strings written to the authentication request log file are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the authentication request log entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteTime</td>
<td>■ If set to 1, time and date values written to the authentication request log file are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the authentication request log entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>RollOver</td>
<td>Specifies how often the current authentication request log file is closed and a new file opened (a rollover), up to one rollover per minute.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, the authentication request log rolls over once every 24 hours, at midnight local time.</td>
</tr>
<tr>
<td></td>
<td>■ If set to a number in the range 1–1440, specifies the number of minutes until the next rollover.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>RollOverOnStartup</td>
<td>■ If set to 1, each time Steel-Belted Radius is started, it closes the current authentication request log file and opens a new one. A sequence number _nnnnn is appended to the log file name, just as when MaxSize is reached.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, each time Steel-Belted Radius is started, it appends entries to the previously open authentication request log file.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>Titles</td>
<td>■ If set to 1, each time a new authentication request log file is created, the title line (containing column headings) is written to the file.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, the line is not written.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>UTC</td>
<td>■ If set to 1, time and date values are provided according to universal time coordinates (UTC, formerly known as Greenwich mean time or GMT).</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, time and date values reflect local time.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
</tbody>
</table>
authReport.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The authReport.ini initialization file controls whether Steel-Belted Radius generates the following reports:

- Authentication acceptance report
- Authentication rejection report
- Unknown authentication client report
- Invalid shared secret report

If enabled, these reports are written to the `radiusdir\authReports` directory on the Steel-Belted Radius server.

**NOTE:** The settings in the authReport.ini file are overwritten when the SBR Administrator is used to enable or disable these reports.

### [AcceptReport] Section

The [AcceptReport] section of authReport.ini (Table 32) enables or disables generation of the authentication acceptance report. The settings for the authentication acceptance report are specified in the authReportAccept.ini file, which is described on page 75.

Sample syntax is as follows:

```
[AcceptReport]
Enable = 1
```

**Table 32: authReport.ini [AcceptReport] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | ■ If set to 1, Steel-Belted Radius periodically generates the authentication acceptance report.  
 |           | ■ If set to 0, the authentication acceptance report is not generated.  
 |           | Default value is 1. |

### [BadSharedSecretReport] Section

The [BadSharedSecretReport] section of authReport.ini (Table 33) enables or disables generation of the invalid shared secret report. The settings for the invalid shared secret report are specified in the authReportBadSharedSecret.ini file, which is described on page 78.

Sample syntax is as follows:
[BadSharedSecretReport]
Enable = 1

Table 33: authReport.ini [BadSharedSecretReport] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | ▪ If set to 1, Steel-Belted Radius periodically generates the invalid shared secret report.  
            ▪ If set to 0, the invalid shared secret report is not generated.  
            Default value is 1. |

[RejectReport] Section

The [RejectReport] section of authReport.ini (Table 34) enables or disables generation of the authentication rejection report. The settings for the authentication rejection report are specified in the authReportReject.ini file, which is described on page 81.

Sample syntax is as follows:

[RejectReport]
Enable = 1

Table 34: authReport.ini [RejectReport] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | ▪ If set to 1, Steel-Belted Radius periodically generates the authentication rejection report.  
            ▪ If set to 0, the authentication rejection report is not generated.  
            Default value is 1. |

[UnknownClientReport] Section

The [UnknownClientReport] section of authReport.ini (Table 35) enables or disables generation of the unknown authentication client report. The settings for the unknown authentication client report are specified in the authReportUnknownClient.ini file, which is described on page 85.

Sample syntax is as follows:

[UnknownClientReport]
Enable = 1

Table 35: authReport.ini [UnknownClientReport] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | ▪ If set to 1, Steel-Belted Radius periodically generates the unknown authentication client report.  
            ▪ If set to 0, the unknown authentication client report is not generated.  
            Default value is 1. |
authReportAccept.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The authReportAccept.ini initialization file specifies options for the authentication acceptance report, which is an ASCII comma-delimited file that contains information about successful authentications by the Steel-Belted Radius server.

### [Attributes] Section

The [Attributes] section of authReportAccept.ini lists the attributes logged in the acceptance log.

You can configure what is logged to the acceptance report by entering attributes in the [Attributes] section in the sequence in which they should appear. This lets you design the content and column order of any spreadsheets that you plan to create based upon the acceptance report.

The syntax of the [Attributes] section is as follows:

```
[Attributes]
AttributeName=
AttributeName=

For example:

[Attributes]
User-Name=
NAS-IP-Address=
```

The [Attributes] section lists one `AttributeName` on each line. You must ensure that an equal sign (=) immediately follows each `AttributeName`, with no spaces in between. Improperly formatted entries are considered invalid and are ignored.

Each `AttributeName` in the [Attributes] section must be defined in a standard RADIUS or vendor-specific dictionary file (.dct) installed on the Steel-Belted Radius server.

**NOTE:** The first four attributes in each acceptance report entry (Date, Time, RAS-Client, and Full-Name) are always enabled, and cannot be re-ordered or deleted. Therefore, these attributes do not appear in the [Attributes] section of the authReportAccept.ini file.

### [Settings] Section

The [Settings] section of authReportAccept.ini (Table 36) specifies the operational characteristics of the authentication acceptance report.
If the `MaxMinutesPerFile` parameter is set to 0, the file name of the authentication acceptance report is `accepts_yyymmdd.csv` (where `yyymmdd` identifies the date the report was generated.) If the `MaxMinutesPerFile` parameter is set to a value greater than 0, the file name of the report is `accepts_yyymmdd_hhmm.csv` (where `yyymmdd` identifies the date and `hhmm` identifies the time the report was generated.)

Sample syntax is as follows:

```
[Settings]
BufferSize = 131072
DaysToKeep = 1
LineSize = 4096
LogFilePermissions = ralphw:1007 rw-r- - - -
MaxMinutesPerFile = 0
QuoteInteger = 1
QuoteIpAddress = 1
QuoteBinary = 1
QuoteText = 1
QuoteTime = 1
UTC = 0
```

### Table 36: authReportAccept.ini [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>BufferSize</td>
<td>The size of the buffer used in the logging process, in bytes. Default value is 131072.</td>
</tr>
<tr>
<td>DaysToKeep</td>
<td>Specifies the number of days the Steel-Belted Radius server should retain each authentication acceptance report. Default value is 1 (one day).</td>
</tr>
<tr>
<td>LineSize</td>
<td>The maximum size of a single log line. The allowable range is 1024 to 32768. Default value is 4096.</td>
</tr>
<tr>
<td>LogFilePermissions</td>
<td>Specifies the owner and access permission setting for the authentication acceptance log (<code>accepts_yyymmdd.csv</code>) file. Enter a value for the LogFilePermissions setting in <code>owner:group permissions</code> format, where:</td>
</tr>
<tr>
<td></td>
<td>- <strong>owner</strong> specifies the owner of the file in text or numeric format.</td>
</tr>
<tr>
<td></td>
<td>- <strong>group</strong> specifies the group setting for the file in text or numeric format.</td>
</tr>
<tr>
<td></td>
<td>- <strong>permissions</strong> specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format. For example, <code>ralphw:1007 rw-r-- - - - -</code> specifies that the file owner (<code>ralphw</code>) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and that other users cannot access the log file.</td>
</tr>
<tr>
<td>MaxMinutesPerFile</td>
<td>Specifies how often the current authentication acceptance report is closed and a new file opened.</td>
</tr>
<tr>
<td></td>
<td>- If set to <code>n</code> (where <code>n</code> is a number greater than 0), a new report is generated every <code>n</code> minutes.</td>
</tr>
<tr>
<td></td>
<td>- If set to 0, a new report is generated once every 24 hours, at midnight local time.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
</tbody>
</table>

**NOTE:** The value entered for `MaxMinutesPerFile` determines the file name of the generated report.
Table 36: authReportAccept.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| QuoteBinary  | - If set to 1, binary values written to the report are enclosed in quotes.  
               - If set to 0, quotes are not used.  
               Set this value according to the format expected by the application that processes the entries.  
               Default value is 1. |
| QuotInteger  | - If set to 1, integer values written to the report are enclosed in quotes.  
               - If set to 0, quotes are not used.  
               Set this value according to the format expected by the application that processes the entries.  
               Default value is 1. |
| QuoteIPAddress | - If set to 1, IP addresses written to the report are enclosed in quotes.  
               - If set to 0, quotes are not used.  
               Set this value according to the format expected by the application that processes the entries.  
               Default value is 1. |
| QuoteText    | - If set to 1, text strings written to the report are enclosed in quotes.  
               - If set to 0, quotes are not used.  
               Set this value according to the format expected by the application that processes the entries.  
               Default value is 1. |
| QuoteTime    | - If set to 1, time and date values written to the report are enclosed in quotes.  
               - If set to 0, quotes are not used.  
               Set this value according to the format expected by the application that processes the entries.  
               Default value is 1. |
| UTC          | - If set to 1, time and date values are provided according to universal time coordinates (UTC, formerly known as Greenwich mean time or GMT).  
               - If set to 0, time and date values reflect local time.  
               Default value is 0. |
authReportBadSharedSecret.ini File

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE
Not Used By: —

The authReportBadSharedSecret.ini initialization file specifies options for the invalid shared secret report, which is an ASCII comma-delimited file that records information about requests received from known RADIUS clients that used an invalid shared secret. This condition is only detectable if the authentication request contained a Message-Authenticator attribute, which is required if credentials are of an EAP type but optional if credentials are PAP, CHAP, or MS-CHAP. (In the case of PAP, an invalid shared secret will not be detected, but will result in an Access-Reject response as the user password is decrypted into incorrect characters.)

If the MaxMinutesPerFile parameter is set to 0, the file name of the bad shared secret report is `badSharedSecret_yyyymmdd.csv` (where `yyyymmdd` identifies the date the report was generated.) If the MaxMinutesPerFile parameter is set to a value greater than 0, the file name of the report is `badSharedSecret_yyyymmdd_hhmm.csv` (where `yyyymmdd` identifies the date and `hhmm` identifies the time the report was generated).

[Attributes] Section

The [Attributes] section of authReportBadSharedSecret.ini lists the attributes logged in the invalid shared secret report.

You can configure what is logged to the invalid shared secret report by entering attributes in the [Attributes] section in the sequence in which they should appear. This lets you design the content and column order of any spreadsheets that you plan to create based upon the silent discard/bad shared secret report.

The syntax of the [Attributes] section is as follows:

```
[Attributes]
AttributeName=
AttributeName=
```

For example:

```
[Attributes]
User-Name=
NAS-IP-Address=
```

The [Attributes] section lists one `AttributeName` on each line. You must ensure that an equal sign (`=`) immediately follows each `AttributeName`, with no spaces in between. Improperly formatted entries are ignored.
Each **AttributeName** in the [Attributes] section must be defined in a standard RADIUS or vendor-specific dictionary file (.dct) installed on the Steel-Belted Radius server.

---

**NOTE:** The first three attributes in each invalid shared secret report entry (Date, Time, and RADIUS-Client) are always enabled, and cannot be re-ordered or deleted. Therefore, these attributes do not appear in the [Attributes] section of the authReportBadSharedSecret.ini file.

### [Settings] Section

The [Settings] section of authReportBadSharedSecret.ini specifies the operational characteristics of the invalid shared secret report. Sample syntax is as follows:

```
[Settings]
BufferSize = 131072
DaysToKeep = 1
LineSize = 4096
LogFilePermissions = ralphw:1007 rw-r- - - - -
MaxMinutesPerFile = 0
QuoteBinary = 1
QuoteInteger = 1
QuoteIpAddress = 1
QuoteText = 1
QuoteTime = 1
UTC = 0
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>BufferSize</td>
<td>The size of the buffer used in the logging process, in bytes. Default value is 131072.</td>
</tr>
<tr>
<td>DaysToKeep</td>
<td>Specifies the number of days the Steel-Belted Radius server should retain each invalid shared secret report. Default value is 1 (one day).</td>
</tr>
<tr>
<td>LineSize</td>
<td>The maximum size of a single log line. The allowable range is 1024 to 32768. Default value is 4096.</td>
</tr>
</tbody>
</table>
| LogFilePermissions (Solaris/Linux only) | Specifies the owner and access permission setting for the invalid shared secret report (badSharedSecret_yyyyMMdd.csv) file. Enter a value for the LogFilePermissions setting in owner:group permissions format, where:  
  - **owner** specifies the owner of the file in text or numeric format.  
  - **group** specifies the group setting for the file in text or numeric format.  
  - **permissions** specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format.  
  
For example, ralphw:1007 rw-r- - - - - specifies that the file owner (ralphw) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and that other users cannot access the log file. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxMinutesPerFile</td>
<td>Specifies how often the current report is closed and a new file opened.</td>
</tr>
<tr>
<td></td>
<td>■ If set to ( n ) (where ( n ) is a number greater than 0), a new report file is generated every ( n ) minutes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, a new report file is generated once every 24 hours, at midnight local time.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The value entered for <code>MaxMinutesPerFile</code> determines the file name of the generated report.</td>
</tr>
<tr>
<td>QuoteBinary</td>
<td>■ If set to 1, binary values written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteInteger</td>
<td>■ If set to 1, integer values written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteIPAddress</td>
<td>■ If set to 1, IP addresses written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteText</td>
<td>■ If set to 1, text strings written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteTime</td>
<td>■ If set to 1, time and date values written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>UTC</td>
<td>■ If set to 1, time and date values are provided according to universal time coordinates (UTC, formerly known as Greenwich mean time or GMT).</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, time and date values reflect local time.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
</tbody>
</table>
authReportReject.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The authReportReject.ini initialization file specifies options for the authentication rejection report, which is an ASCII comma-delimited file that records authentication rejections.

If the MaxMinutesPerFile parameter is set to 0, the file name of the authentication rejection report is `rejects_yyyymmdd.csv` (where `yyyymmdd` identifies the date the report was generated.) If the MaxMinutesPerFile parameter is set to a value greater than 0, the file name of the report is `rejects_yyyymmdd_hhmm.csv` (where `yyyymmdd` identifies the date and `hhmm` identifies the time the report was generated).

**[Attributes] Section**

The [Attributes] section of authReportReject.ini lists the attributes logged in the authentication rejection report.

You can configure what is logged to the authentication rejection report by entering attributes in the [Attributes] section in the sequence in which they should appear. This lets you design the content and column order of any spreadsheets that you plan to create based upon the reject report.

The syntax of the [Attributes] section is as follows:

```ini
[Attributes]
AttributeName=
AttributeName=

;  
```

For example:

```ini
[Attributes]
Service-Type=
Source-IP-Address=
Source-UDP-Port=
```

The [Attributes] section lists one **AttributeName** on each line. You must ensure that an equal sign (=) immediately follows each **AttributeName**, with no spaces in between. Improperly formatted entries are ignored.

Each **AttributeName** in the [Attributes] section must be defined in a standard RADIUS or vendor-specific dictionary file (.dct) installed on the Steel-Belted Radius server.

The following attributes in each authentication rejection report entry are always enabled, and cannot be re-ordered or deleted:

- **Date** – Identifies the date of the authentication rejection.
- **Time** – Identifies the time of the authentication rejection.
- **RADIUS-Client** – Identifies the RADIUS client that received the authentication rejection.
- **User-Name** – Identifies the name of the user that was rejected.
- **Reject-Method** – Identifies the most relevant authentication method that rejected the user. If this information is unavailable, the parameter is set to **Unknown**.
- **Reject-Reason** – Identifies one of the following reasons for the authentication rejection:
  - System error
  - Blacklisted user
  - Invalid request
  - Database or directory not available
  - User not in database
  - Credentials invalid
  - User name or credential incorrect
  - Post-processing error
  - Unknown
- **Reject-Log** – Identifies the reason for the authentication request in language supplied by the authentication method. If a reason is not supplied, the parameter is set to **Unavailable**.

These attributes do not appear in the [Attributes] section of the **authReportReject.ini** file.

### [Settings] Section

The [Settings] section of **authReportReject.ini** specifies the operational characteristics of the authentication rejection report. Sample syntax is as follows:

```
[Settings]
UTC = 0
BufferSize = 131072
MaxMinutesPerFile = 0
DaysToKeep = 1
LineSize = 4096
LogfilePermissions = ralphw:1007 rw-r- ----
QuoteInteger = 1
QuoteIpAddress = 1
QuoteText = 1
QuoteTime = 1
QuoteBinary = 1
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>BufferSize</td>
<td>Specifies the size of the buffer used in the logging process, in bytes.</td>
</tr>
<tr>
<td></td>
<td>Default value is 131072.</td>
</tr>
</tbody>
</table>
### Table 38: `authReportReject.ini` [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DaysToKeep</td>
<td>Specifies the number of days the Steel-Belted Radius server should retain each rejection report. Default value is 1 (one day).</td>
</tr>
<tr>
<td>LineSize</td>
<td>Specifies the maximum size of a single log line. The allowable range is 1024 to 32768. Default value is 4096.</td>
</tr>
<tr>
<td>LogFilePermissions</td>
<td>Specifies the owner and access permission setting for the authentication rejection report (<code>rejects_yyymmd.csv</code>) file. Enter a value for the LogFilePermissions setting in <code>owner:group permissions</code> format, where:</td>
</tr>
<tr>
<td></td>
<td>- <code>owner</code> specifies the owner of the file in text or numeric format.</td>
</tr>
<tr>
<td></td>
<td>- <code>group</code> specifies the group setting for the file in text or numeric format.</td>
</tr>
<tr>
<td></td>
<td>- <code>permissions</code> specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format. For example, <code>ralphw:1007 rw-r- - - -</code> specifies that the file owner (<code>ralphw</code>) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and that other users cannot access the log file.</td>
</tr>
<tr>
<td>MaxMinutesPerFile</td>
<td>Specifies how often the current report is closed and a new file opened.</td>
</tr>
<tr>
<td></td>
<td>- If set to <code>n</code> (where <code>n</code> is a number greater than 0), a new report file is generated every <code>n</code> minutes.</td>
</tr>
<tr>
<td></td>
<td>- If set to 0, a new report file is generated once every 24 hours, at midnight local time.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The value entered for <code>MaxMinutesPerFile</code> determines the file name of the generated report.</td>
</tr>
<tr>
<td>QuoteBinary</td>
<td>If set to 1, binary values written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteInteger</td>
<td>If set to 1, integer values written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteIPAddress</td>
<td>If set to 1, IP addresses written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteText</td>
<td>If set to 1, text strings written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
</tbody>
</table>
Table 38: authReportReject.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| QuoteTime | If set to 1, time and date values written to the report are enclosed in quotes.  
|           | If set to 0, quotes are not used.  
|           | Set this value according to the format expected by the application that processes the entries.  
|           | Default value is 1. |

| UTC       | If set to 1, time and date values are provided according to universal time coordinates (UTC, formerly known as Greenwich mean time or GMT).  
|           | If set to 0, time and date values reflect local time.  
|           | Default value is 0. |
authReportUnknownClient.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The authReportUnknownClient.ini initialization file specifies options for the unknown authentication client report, which is an ASCII comma-delimited file produced by the Steel-Belted Radius server that identifies requests received from unknown RADIUS clients.

If the **MaxMinutesPerFile** parameter is set to 0, the file name of the unknown authentication client report is `unknownClient_yyyyMMdd.csv` (where `yyyyMMdd` identifies the date the report was generated.) If the **MaxMinutesPerFile** parameter is set to a value greater than 0, the file name of the report is `unknownClient_yyyyMMdd_hhmm.csv` (where `yyyyMMdd` identifies the date and `hhmm` identifies the time the report was generated.)

**[Attributes] Section**

The [Attributes] section of authReportUnknownClient.ini lists the attributes logged in the unknown client report.

You can configure what is logged to the unknown client log by entering attributes in the [Attributes] section in the sequence in which they should appear. This lets you design the content and column order of any spreadsheets that you plan to create based upon the unknown client log.

The syntax of the [Attributes] section is as follows:

```
[Attributes]
AttributeName=
AttributeName=
;
```

For example:

```
[Attributes]
User-Name=
```

The [Attributes] section lists one **AttributeName** on each line. You must ensure that an equal sign (=) immediately follows each **AttributeName**, with no spaces in between. Improperly formatted entries are considered invalid and are ignored.

Each **AttributeName** in the [Attributes] section must be defined in a standard RADIUS or vendor-specific dictionary file (.dct) installed on the Steel-Belted Radius server.

**NOTE:** The first six attributes in each unknown client report entry (Date, Time, Source-IP-Address, Source-UDP-Port, Target-IP-Address, and Target-UDP-Port) are always enabled, and cannot be re-ordered or deleted. Therefore, these attributes do not appear in the [Attributes] section of the authReportUnknownClient.ini file.
[Settings] Section

The [Settings] section of authReportUnknownClient.ini specifies the operational characteristics of the unknown authentication client report. Sample syntax is as follows:

```
[Settings]
BufferSize = 131072
DaysToKeep = 1
LineSize = 4096
LogFilePermissions = ralphw:1007 rw-r--
MaxMinutesPerFile = 0
QuoteBinary = 1
QuoteInteger = 1
QuoteIpAddress = 1
QuoteText = 1
QuoteTime = 1
UTC = 0
```

Table 39: authReportUnknownClient.ini [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>BufferSize</td>
<td>The size of the buffer used in the logging process, in bytes. Default value is 131072.</td>
</tr>
<tr>
<td>DaysToKeep</td>
<td>Specifies the number of days the Steel-Belted Radius server should retain each unknown client report. Default value is 1 (one day).</td>
</tr>
<tr>
<td>LineSize</td>
<td>The maximum size of a single log line. The allowable range is 1024 to 32768. Default value is 4096.</td>
</tr>
</tbody>
</table>
| LogFilePermissions | Specifies the owner and access permission setting for the unknown authentication client report (unknownClient_yyyymmdd_hhmm.csv) file. Enter a value for the LogFilePermissions setting in owner:group permissions format, where:
- **owner** specifies the owner of the file in text or numeric format.
- **group** specifies the group setting for the file in text or numeric format.
- **permissions** specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format.
For example, ralphw:1007 rw-r-- specifies that the file owner (ralphw) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and that other users cannot access the log file. |
| MaxMinutesPerFile | Specifies how often the current report is closed and a new file opened.
- If set to $n$ (where $n$ is a number greater than 0), a new report file is generated every $n$ minutes.
- If set to 0, a new report file is generated once every 24 hours, at midnight local time. Default value is 0.
**NOTE:** The value entered for MaxMinutesPerFile determines the file name of the generated report. |
Table 39: authReportUnknownClient.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>QuoteBinary</td>
<td>If set to 1, binary values written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that</td>
</tr>
<tr>
<td></td>
<td>processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteInteger</td>
<td>If set to 1, integer values written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that</td>
</tr>
<tr>
<td></td>
<td>processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteIPAddress</td>
<td>If set to 1, IP addresses written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that</td>
</tr>
<tr>
<td></td>
<td>processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteText</td>
<td>If set to 1, text strings written to the report are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that</td>
</tr>
<tr>
<td></td>
<td>processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteTime</td>
<td>If set to 1, time and date values written to the report are enclosed in</td>
</tr>
<tr>
<td></td>
<td>quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the application that</td>
</tr>
<tr>
<td></td>
<td>processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>UTC</td>
<td>If set to 1, time and date values are provided according to universal</td>
</tr>
<tr>
<td></td>
<td>time coordinates (UTC, formerly known as Greenwich mean time or GMT).</td>
</tr>
<tr>
<td></td>
<td>If set to 0, time and date values reflect local time.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
</tbody>
</table>
**blacklist.ini File**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

The `blacklist.ini` configuration file enables and configures blacklist settings. Only one profile can be created for the purposes of blacklisting, and any login attempt that matches that profile is blocked. An authentication request matches the blacklist profile if the attributes in the request match the checklist attributes of the profile. The profile can contain multiple attributes, and if any of the attributes match those of the profile, the attempt is rejected.

The `blacklist.ini` file contains one configuration section called `[Settings]` (Table 40), which has the following settings:

```plaintext
[Settings]
Enable = <0|1>
IncludeProxy = <0|1>
Profile = profile
```

**Table 40: blacklist.ini Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable     | ■ If set to 1, blacklisting is enabled.  
            | ■ If set to 0, blacklisting is disabled.  
            | Default value is 0. |
| IncludeProxy | ■ If set to 1, blacklisting is configured to include proxy requests, meaning that it is applied to all authentication requests.  
              | ■ If set to 0, blacklisting is configured only to local authentication requests.  
              | Default value is 0. |
| Profile     | Specifies the name of the blacklist profile in the Steel-Belted Radius database. |

The following example enables the blacklist feature and specifies Steel-Belted Radius should use the BlockedNumbers profile to filter authentication requests.

```plaintext
[Settings]
Enable = 1
IncludeProxy = 0
Profile = BlockedNumbers
```

The `BlockedNumbers` profile called by this `blacklist.ini` file specifies checklist attributes Steel-Belted Radius uses to reject authentication requests. The following entries in the `BlockedNumbers` profile identify Calling-Station-Id phone numbers used by rogue users you want to block.

```plaintext
Calling-Station-Id = 617-999-9119  
Calling-Station-Id = 800-515-7889
```
**lockout.ini File**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

The lockout.ini configuration file enables and configures account lockout settings. Account lockout lets you disable an account after a configurable number of failed login attempts within a configurable period. For example, if a user enters an incorrect password three times within two minutes, Steel-Belted Radius can lock out the user’s account temporarily. During the lockout period, the user cannot log in, even with the correct password. Attempts to authenticate against a locked out account cause Steel-Belted Radius to respond with an Access-Reject message immediately.

The lockout.ini file contains one configuration section called [Settings], which has settings similar to the following:

```
[Settings]
Enable = 0
Rejects = 3
Within = 120
Lockout = 600
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | If set to 0, lockout is disabled.  
If set to 1, lockout is enabled.  
Default value is 0. |
| Lockout   | Specifies the lockout period in seconds.  
Default value is 600 seconds (10 minutes). |
| Rejects   | Specifies the number of rejected attempts prior to lockout.  
Default value is 3. |
| Within    | Specifies the period in seconds during which a specified number of rejects causes a lockout.  
Default value is 120 seconds (two minutes). |

**NOTE:** If you enable the lockout facility in Steel-Belted Radius and you use a tunneled authentication method (TTLS or PEAP) with a prefetch-capable method (native user, SQL, or LDAP) and an enabled EAP protocol (MS-CHAPv2, MD5-Challenge, LEAP, TLS), then you must enable Handle via Auto-EAP First in that prefetch-capable method to prevent the outer username (anonymous) from being added to the lockout list.

Otherwise, when Steel-Belted Radius receives an authentication request that uses an unconfigured EAP method, Steel-Belted Radius will reject the user (because the EAP method is not configured) and add the outer username (anonymous) to its lockout list. This will result in all users with an outer authentication name of anonymous being rejected until the lockout period expires.
redirect.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

Account redirection lets you flag an account for special processing after a configurable number of failed login attempts within a configurable time period. The *redirect.ini* initialization file specifies the settings used for account redirection when users forget or mis-enter their passwords.

**[Settings] Section**

The [Settings] section of *redirect.ini* (Table 42) enables and configures account redirection settings.

### Table 42: *redirect.ini* [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | - If set to 0, account redirection is disabled.  
|           | - If set to 1, account redirection is enabled.  
|           | *NOTE:* Account redirection and account lockout are incompatible. Do not enable account redirection if account lockout is enabled.  
| Lockout   | The number of seconds in the account redirection lockout period. For example, a lockout period of 86,400 seconds locks a user out for one day if account redirection processing fails to authenticate the user.  
|           | Default value is 600 seconds (10 minutes).  
| Profile   | The name of the global profile that supplies the values and attributes used for the user after account redirection is triggered.  
|           | Default value is Redirect.  
| Redirect  | The number of seconds during which a user is in redirect state. If the redirection period elapses without another user authentication request, the user is returned to normal state.  
|           | Default value is 120 seconds.  
| Rejects   | The number of rejected attempts prior to redirection.  
|           | Default value is 3.  
| Within    | The period in seconds during which a specified number of rejects causes account redirection.  
|           | Default value is 180 seconds (3 minutes).  

For example, the following [Settings] section of *redirect.ini* specifies that, if a user fails authentication three times within 180 seconds, the user account is placed into redirect state. If the user does not submit another authentication request within 120 seconds of entering redirect state, the user account is restored to normal state.

```
[Settings]
Enable = 0
Rejects = 3
Within = 180
Redirect = 120
```
Profile = RedirectProfile
Lockout = 86400

If the user submits another authentication request within 120 seconds of entering redirect state, the user is accepted without authentication or authorization processing, the user’s account is placed into accept-pending state, and the RADIUS accept message for the user contains the values and attributes specified in the global RedirectProfile profile. (These values or attributes could be used by an external customer process to direct the user to a secure web page that asks for alternative authentication information or billing information; the external process might then mail the user an access password if the user satisfies the external process requirements.)

When a user is in accept-pending state, the user’s next authentication request determines whether Steel-Belted Radius accepts or locks out the user:

- If the next authentication is successful, the user account is returned to normal state.
- If the next authentication fails to accept the user, the user account is locked out for 86,400 seconds (one day). During this lockout period, authentication requests for this user are rejected automatically, even if the user enters the correct password.

[ClientExclusionList] Section

The [ClientExclusionList] section of redirect.ini identifies the RADIUS clients that are excluded from account redirection processing. Each entry in the [ClientExclusionList] section of redirect.ini consists of the name of a RADIUS client device, as configured in the Steel-Belted Radius database.
securid.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The securid.ini file lets you replace the default prompt strings used in RSA SecurID authentication with customized strings. Customized prompt strings are useful in situations where authentication is to be performed by means of RSA SecurID and the default prompt strings are too long for the screen on the authentication device.

If the securid.ini file is present in the Steel-Belted Radius server directory, Steel-Belted Radius uses prompt strings specified in the file instead of the default prompt strings. Sets of strings can be substituted in whole or in part. If a string is not represented by an entry in the securid.ini file, Steel-Belted Radius uses the default prompt string.

**[Configuration] Section**

The [Configuration] section of securid.ini specifies RSA SecurID access settings.

```
[Configuration]
Enable = 1
AllowSystemPins = 0
CheckUserAllowedByClient = 1
DefaultProfile = DEFAULT
```

**Table 43: securid.ini [Configuration] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable                        | ■ If set to 1, Steel-Belted Radius can authenticate users by means of RSA SecurID.  
|                               | ■ If set to 0, Steel-Belted Radius cannot authenticate users by means of RSA SecurID.  
|                               | Default value is 1.                                                      |
| AllowSystemPins               | ■ If set to 1, users who are configured in the RSA Authentication Manager to receive a system-generated PIN when in New PIN mode are accepted.  
|                               | ■ If set to 0, users who are configured in the RSA Authentication Manager to receive system-generated PIN when in New PIN mode are rejected.  
|                               | Default value is 0.                                                     |
| CheckUserAllowedByClient      | ■ If set to 1, the RADIUS server verifies the user is allowed to connect through the network access device.  
|                               | ■ If set to 0, the RADIUS server does not verify the user is allowed to connect through the network access device.  
|                               | Default value is 1.                                                     |
|                               | **NOTE:** If this parameter is set to 1, RADIUS clients must be configured as Agent Hosts in RSA Authentication Manager. |
| DefaultProfile                | Default profile to be assigned to a user if the RSA Authentication Manager does not return a profile.  
|                               | Default value is DEFAULT.                                               |
**[Server_Settings] Section**

The [Server_Settings] section of securid.ini specifies settings for Extended One-Time Password (EOTP or EAP-15) and Protected One-Time Password (POTP or EAP-32) authentication.

```
[Server_Settings]
Greeting =
Return_MPPE_Keys = 1
```

**Table 44: securid.ini [Configuration] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greeting</td>
<td>A string of as many as 80 characters returned to a network access device after a user is authenticated. For example, &quot;Welcome to RSA Security Software.&quot;</td>
</tr>
</tbody>
</table>
| Return_MPPE_Keys   | ■ If set to 0, the module does not forward RADIUS MS-MPPE Send-Key and MS-MPPE-Recv-Key attributes.  
                      ■ If set to 1, the module includes RADIUS MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes in the final RADIUS Access-Accept response sent to the Access Point. This is necessary for the Access Point to key the WEP encryption.  
                      If the Access Point is authenticating only end users and WEP is not being used, this attribute may be set to 0.  
                      Default value is 1. |

**[Prompts] Section**

If the securid.ini file is present in the Steel-Belted Radius server directory, Steel-Belted Radius uses prompt strings specified in the file instead of the default prompt strings. Sets of strings can be substituted in whole or in part. If a string is not represented by an entry in the securid.ini file, Steel-Belted Radius uses the default prompt string.

**Substitution String Formats**

Substitution strings use %s to mark locations at which variable text is to be substituted. Strings can have no %s placeholders, exactly one %s placeholder, or exactly two %s placeholders. When writing your own prompt strings, you must supply strings with the expected number of %s placeholders. String names include a reminder suffix that reflects the number of %s placeholders:

- Strings that require two %s placeholders have names with a _S_S suffix. The first %s placeholder typically presents a number range (“4 to 8”). The second %s placeholder specifies “characters” or “digits” (or the equivalent, as configured in the Characters and Digits settings).

- Strings that require one %s placeholder have names with a _S suffix. The %s placeholder is replaced with a system-generated PIN.

- Strings that do not require %s placeholders have names with no suffix.

If a string in the securid.ini file is formatted incorrectly, it is ignored and the default prompt string is used.
Table 45 lists formatting conventions for the securid.ini file.

**Table 45: Substitution String Formatting Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>\b</td>
<td>Backspace; not typically used</td>
</tr>
<tr>
<td>\f</td>
<td>Formfeed</td>
</tr>
<tr>
<td>\n</td>
<td>Newline; typically used in conjunction with \r</td>
</tr>
<tr>
<td>\r</td>
<td>Carriage return; typically used in conjunction with \n</td>
</tr>
<tr>
<td>\t</td>
<td>Horizontal tab</td>
</tr>
<tr>
<td>\v</td>
<td>Vertical tab; not typically used</td>
</tr>
<tr>
<td>\</td>
<td>Displayed backslash</td>
</tr>
<tr>
<td>&quot;</td>
<td>Displayed double-quote character</td>
</tr>
<tr>
<td>’</td>
<td>Displayed single-quote character</td>
</tr>
</tbody>
</table>

If other characters in a substitution string are preceded by a backslash, the backslash is ignored and the character is displayed unchanged.

**Quoted Strings**

Trailing white space is ignored when an unquoted prompt string is read into Steel-Belted Radius. If you want a substitution string to include trailing white space, insert double-quote marks at the beginning and end of the string, enclosing the white space you want to include. For example, if you want a string to be displayed as the word *PIN* followed by a colon followed by a single space, you would enter `StringName="PIN: "` (with a space between the colon and the closing double-quote character).

**Example 1: Verbose Substitution Strings**

Figure 1 lists the default prompt strings, which may be too long for some SecurID displays. Although text lines in this display appear to wrap to a second line, text wrapping is not supported in securid.ini entries.
Chapter 3: Authentication Configuration Files

Figure 1 Verbose Substitution Strings

Example 2: 2 x 40 Display Substitution Strings

Figure 2 displays prompt strings designed for a 2 line x 40 character display. Although text lines in this display appear to wrap to a second line, text wrapping is not supported in securid.ini entries.
Figure 2 2x50 Display Substitution Strings

Example 3: Terse Substitution Strings

Figure 3 displays prompt strings designed to be parsed by a program at the client endpoint rather than read by a user.
; BEGINNING OF extremely terse prompts. These are appropriate for automatic
; interpretation by another program which parses the prompts. A well trained
; end user could use these.
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;[Prompts]
;InputNextCode        = Next code
;InputMustChoose_S_S  = Must choose
;InputCannotChoose    = Cannot choose
;InputMayChoose_S_S   = May choose (%s, %s)
;InputReadyForPin     = Ready for pin
;InputReadyForPin_1_S = Ready for pin 1
;InputReenterPin      = Reenter pin
;InputReenterPin_1    = Reenter pin 1
;OutputReject         = Reject
;OutputChange         = Change
;OutputAccepted       = Accepted
;OutputDenied         = Denied
;OutputNoPassReqd     = No pass reqd
;OutputDeniedFinal    = Denied final
;Characters           = chars
;Digits               = digits
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;

Figure 3 Terse Substitution Strings


**statlog.ini File**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The `statlog.ini` initialization file configures the Steel-Belted Radius statistics log file (`yyyyymmdd.statlog`), which periodically records server statistics to a comma-delimited ASCII file. The statistics log provides a mechanism for creating snapshots of user-selected server statistics.

- The first line in a `*.statlog` file lists all column headings in double quotes ("Date", "Time", ...).

- The first column in a `*.statlog` file identifies the current date in `yyyy-mm-dd` format in double-quotes ("2006-02-13"). The `*.statlog` file uses the local date, not the date in the UTC time zone, when it records date information.

- The second column in a `*.statlog` file identifies the current time in `hh:mm:ss` format in double-quotes ("14:13:22"). The `*.statlog` file uses the local time, not the time in the UTC time zone, when it records time information.

- If statistics logging is enabled, a new statistics logging file is created the first time the server is started each day. At midnight, the server closes the old statistics log file and starts a new one with a file name that reflects the new date.

- If you restart the Steel-Belted Radius server and a `*.statlog` file exists for the current day, the server appends new information to the existing `*.statlog` file. When the server is restarted, the timer for capturing statistics snapshots is restarted; for example, a server configured to record statistics every 10 minutes captures statistics at 14:10:00. If the server is restarted at 14:15:00, it captures system statistics immediately (14:15:00) and 10 minutes thereafter (14:25:00); it does not try to capture statistics at 14:20:00 (10 minutes after the capture before the restart).

- If you change the order or contents of the list of statistics to be recorded and restart the server, Steel-Belted Radius detects the change and writes an entry with the new column headers to the current `*.statlog` file before writing new data records into the file.

---

**NOTE:** When you change the order or contents of the list of statistics recorded in the `*.statlog` file, Steel-Belted Radius creates the `statloghdr.dat` checkpoint file in the `radiusdir` directory. Do not modify or delete the `statloghdr.dat` file.

---

**[Settings] Section**

The [Settings] section of `statlog.ini` (Table 48) specifies whether the statistics log file is enabled, who can access the statistics log file, how frequently the server writes information to the statistics log file, and the number of days statistics log files are retained.
Chapter 3: Authentication Configuration Files

Table 46: statlog.ini.ini [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable             | ■ If set to 1, the Steel-Belted Radius server periodically writes statistics information to the `yyyyymmdd.statlog` file.  
■ If set to 0, the Steel-Belted Radius server does not update the `yyyyymmdd.statlog` file.  
Default value is 0. |
| LogFilePermissions (Solaris/Linux only) | Specifies the owner and access permission setting for the `*.statlog` file.  
Enter a value for the LogFilePermissions setting in `owner:group permissions` format, where:  
■ `owner` specifies the owner of the file in text or numeric format.  
■ `group` specifies the group setting for the file in text or numeric format.  
■ `permissions` specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format.  
For example, `ralphw:1007 rw-r---` specifies that the file owner (`ralphw`) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and other users cannot access the log file. |
| Interval-Seconds   | Specifies the number of seconds (in the range 1–3600) that the Steel-Belted Radius server waits before writing new statistics information to the statistics log.  
Default value is 600 seconds (10 minutes). |
| Days-To-Keep       | Specifies the number of days (in the range 1–365) the statistics log is retained by the Steel-Belted Radius server. When the specified number of days has elapsed, the statistics log is automatically purged.  
Default value is 7 days. |

For example:

```
[Settings]
Enable = 0
;LogFilePermissions = ralphw:1007 rw-r---
;Interval-Seconds = 600
;Days-To-Keep = 7
```

[Statistics] Section

The [Statistics] section of statlog.ini (Table 48) identifies the statistics you want included in the snapshot. Each entry in this section takes the format `Source/Statistic`, where `Source` identifies the LCI statistics container that holds the statistic counter you want and `Statistic` identifies the statistic by name.

Statistics are written to the log file in the order in which they are listed in the [Statistics] section.
### Table 47: statlog.ini.ini [Statistics] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| **Source** | Specifies is the name of the LCI statistics container that holds the specified statistic.  
Supported values for **Source** are:  
- Server  
- Authentication  
- Accounting  
- Proxy  
- Rate |
| **Statistic** | Specifies the name of the statistic you want to record in the log.  
Statistics in the Server LCI container are:  
- Accounting-Threads  
- Authentication-Threads  
- High-Acct-Threads  
- High-Acct-Threads-Since-Reset  
- High-Auth-Threads  
- High-Auth-Threads-Since-Reset  
- High-Total-Threads  
- High-Total-Threads-Since-Reset  
- Max-Acct-Threads  
- Max-Auth-Threads  
- Max-Total-Threads  
- Total-Threads  
Statistics in the Authentication LCI container are:  
- Accept  
- Dropped-Packet  
- Failed-Authentication  
- Failed-On-Check-List  
- Insufficient-Resources  
- Invalid-Request  
- Proxy-Failure  
- Reject  
- Rejected-By-Proxy  
- Silent-Discard  
- Total-Retry-Packets  
- Total-Transactions  
- Transactions-Retried |
(continues)
Table 47: statlog.ini.ini [Statistics] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>(continued)</td>
<td>Statistics in the Accounting LCI container are:</td>
</tr>
<tr>
<td></td>
<td>- Dropped-Packet</td>
</tr>
<tr>
<td></td>
<td>- Insufficient-Resources</td>
</tr>
<tr>
<td></td>
<td>- Interim</td>
</tr>
<tr>
<td></td>
<td>- Invalid-Client</td>
</tr>
<tr>
<td></td>
<td>- Invalid-Request</td>
</tr>
<tr>
<td></td>
<td>- Invalid-Shared-Secret</td>
</tr>
<tr>
<td></td>
<td>- Off</td>
</tr>
<tr>
<td></td>
<td>- On</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Failure</td>
</tr>
<tr>
<td></td>
<td>- Start</td>
</tr>
<tr>
<td></td>
<td>- Stop</td>
</tr>
<tr>
<td></td>
<td>- Total-Retry-Packets</td>
</tr>
<tr>
<td></td>
<td>- Total-Transactions</td>
</tr>
<tr>
<td></td>
<td>- Transactions-Retried</td>
</tr>
</tbody>
</table>

Statistics in the Proxy LCI container are:
- Accounting
- Authentication
- Insufficient-Resources
- Invalid-Response
- Invalid-Shared-Secret
- Timed-Out
- Total-Retry-Packets
- Total-Transactions
- Transactions-Retried

Statistics in the Rate LCI container are:
- Acct-Start-Average-Rate
- Acct-Start-Current-Rate
- Acct-Start-Peak-Rate
- Acct-Stop-Average-Rate
- Acct-Stop-Current-Rate
- Acct-Stop-Peak-Rate
- Auth-Accept-Average-Rate
- Auth-Accept-Current-Rate
- Auth-Accept-Peak-Rate
- Auth-Reject-Average-Rate
- Auth-Reject-Current-Rate
- Auth-Reject-Peak-Rate
- Auth-Request-Average-Rate
- Auth-Request-Current-Rate
- Auth-Request-Peak-Rate

(continues)
Table 47: statlog.ini.ini [Statistics] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>(continued)</td>
<td>Statistics in the Rate LCI container are:</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Acct-Fail-Proxy-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Acct-Fail-Proxy-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Acct-Fail-Proxy-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Acct-Request-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Acct-Request-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Acct-Request-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Rej-Proxy-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Rej-Proxy-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Rej-Proxy-Error-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Rej-Proxy-Error-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Rej-Proxy-Error-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Rej-Proxy-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Request-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Request-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Auth-Request-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Badresp-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Badresp-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Badresp-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Badsecret-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Badsecret-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Missingresr-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Missingresr-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Timeout-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Timeout-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Fail-Timeout-Peak-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Retries-Average-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Retries-Current-Rate</td>
</tr>
<tr>
<td></td>
<td>- Proxy-Retries-Peak-Rate</td>
</tr>
</tbody>
</table>

For example:

```
[Statistics]
Server/Authentication-Threads
Server/Accounting-Threads
Server/Total-Threads
Server/Max-Acct-Threads
Server/Max-Auth-Threads
Server/MaxTotal-Threads
Server/High-Auth-Threads
Server/High-Acct-Threads
Server/High-Total-Threads
Server/High-Acct-Threads-Since-Reset
```
Server/High-Auth-Threads-Since-Reset
Server/High-Total-Threads-Since-Reset

Authentication/Accept
Authentication/Reject
Authentication/Silent-Discard
Authentication/Total-Transactions
Authentication/Dropped-Packet
Authentication/Invalid-Request
Authentication/Failed-Authentication
Authentication/Failed-On-Check-List
Authentication/Insufficient-Resources
Authentication/Proxy-Failure
Authentication/Rejected-By-Proxy
Authentication/Transactions-Retried
Authentication/Total-Retry-Packets

Accounting/Start
Accounting/Stop
Accounting/Interim
Accounting/On
Accounting/Off
Accounting/Total-Transactions
Accounting/Dropped-Packet
Accounting/Invalid-Request
Accounting/Invalid-Client
Accounting/Invalid-Shared-Secret
Accounting/Insufficient-Resources
Accounting/Proxy-Failure
Accounting/Transactions-Retried
Accounting/Total-Retry-Packets

Proxy/Authentication
Proxy/Accounting
Proxy/Total-Transactions
Proxy/Temp-Out
Proxy/Invalid-Response
Proxy/Invalid-Shared-Secret
Proxy/Insufficient-Resources
Proxy/Transactions-Retried
Proxy/Total-Retry-Packets

Rate/Auth-Request-Current-Rate
Rate/Auth-Request-Average-Rate
Rate/Auth-Request-Peak-Rate
Rate/Auth-Accept-Current-Rate
Rate/Auth-Accept-Average-Rate
Rate/Auth-Accept-Peak-Rate
Rate/Auth-Reject-Current-Rate
Rate/Auth-Reject-Average-Rate
Rate/Auth-Reject-Peak-Rate
Rate/Acct-Start-Current-Rate
Rate/Acct-Start-Average-Rate
Rate/Acct-Start-Peak-Rate
Rate/Acct-Stop-Current-Rate
Rate/Acct-Stop-Average-Rate
Rate/Acct-Stop-Peak-Rate
Rate/Proxy-Auth-Request-Current-Rate
Rate/Proxy-Auth-Request-Average-Rate
Rate/Proxy-Auth-Request-Peak-Rate
Rate/Proxy-Acct-Request-Current-Rate
Rate/Proxy-Acct-Request-Average-Rate
Rate/Proxy-Acct-Request-Peak-Rate
Rate/Proxy-Fail-Timeout-Current-Rate
Rate/Proxy-Fail-Timeout-Average-Rate
Rate/Proxy-Fail-Timeout-Peak-Rate
Rate/Proxy-Fail-Badresp-Current-Rate
Rate/Proxy-Fail-Badresp-Average-Rate
Rate/Proxy-Fail-Badresp-Peak-Rate
Rate/Proxy-Fail-Badsecret-Current-Rate
Rate/Proxy-Fail-Badsecret-Average-Rate
Rate/Proxy-Fail-Badsecret-Peak-Rate
Rate/Proxy-Fail-Missingresr-Current-Rate
Rate/Proxy-Fail-Missingresr-Average-Rate
Rate/Proxy-Fail-Missingresr-Peak-Rate
Rate/Proxy-Retries-Current-Rate
Rate/Proxy-Retries-Average-Rate
Rate/Proxy-Retries-Peak-Rate
Rate/Proxy-Auth-Rej-Proxy-Current-Rate
Rate/Proxy-Auth-Rej-Proxy-Average-Rate
Rate/Proxy-Auth-Rej-Proxy-Peak-Rate
Rate/Proxy-Acct-Fail-Proxy-Current-Rate
Rate/Proxy-Acct-Fail-Proxy-Average-Rate
Rate/Proxy-Acct-Fail-Proxy-Peak-Rate
Rate/Proxy-Acct-Fail-Proxy-Average-Rate
Rate/Proxy-Acct-Fail-Proxy-Peak-Rate
Rate/Proxy-Acct-Fail-Proxy-Error-Current-Rate
Rate/Proxy-Acct-Fail-Proxy-Error-Average-Rate
Rate/Proxy-Acct-Fail-Proxy-Error-Peak-Rate
**tacplus.ini File**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The tacplus.ini initialization file provides the configuration information that enables the Steel-Belted Radius server to communicate with a TACACS+ server.

**NOTE:** Steel-Belted Radius does not support the use of IPv6 with TACACS+.

### [ServerInfo] Section

The [ServerInfo] section of tacplus.ini (Table 48) provides information that allows Steel-Belted Radius to communicate with a TACACS+ server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharedSecret</td>
<td>Specifies the shared secret between the TACACS+ server and Steel-Belted Radius</td>
</tr>
<tr>
<td>TargetHost</td>
<td>Specifies the name or IPv4 address of the TACACS+ server.</td>
</tr>
</tbody>
</table>

For example:

```
[ServerInfo]  
SharedSecret=123abc  
TargetHost=197.43.160.101
```
winauth.aut File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE
**Not Used By:** —

The Windows Domain authentication method is configured by means of the `winauth.aut` file.

**[Bootstrap] Section**

The [Bootstrap] section (Table 49) specifies information that Steel-Belted Radius uses to load and start the Windows domain authentication module.

**Table 49: winauth.aut [Bootstrap] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibraryName</td>
<td>Specifies the name of the Windows Domain Authentication module. Default value is <code>winauth.dll</code>. Do not change this unless you are advised to do so by Juniper Customer Support.</td>
</tr>
<tr>
<td>Enable</td>
<td>■ If set to 1, the authentication module is enabled.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, the authentication module is disabled and does not appear in the Authentication Methods list in SBR Administrator. Default value is 1.</td>
</tr>
<tr>
<td>InitializationString</td>
<td>This entry is used to specify the name of the authentication method to appear in the Authentication Methods list in SBR Administrator. Default value is Windows domain authentication. The name of each authentication method must be unique. If you create additional .aut files to implement authentication against multiple databases, be sure that each InitializationString is set to a different method name.</td>
</tr>
</tbody>
</table>

**[WindowsDomain] Section**

The [WindowsDomain] section (Table 50) specifies the server’s response to an expired Domain password. You can choose separate responses for Domain User and Domain Group authentication methods. Steel-Belted Radius takes the actions that you define in the [WindowsDomain] section when it receives an **Expired password** or **User must change password at next logon** status code after passing a username/password pair to a Windows Domain for authentication.

```ini
[WindowsDomain]
AllowExpiredPasswordsForUsers = no
AllowExpiredPasswordsForGroups = no
AllowMachineLogin = yes
PrequalifyChecklist = no
ProfileForExpiredUsers = <place_name_of_Profile_here>
ProfileForExpiredUsersInGroups = <place_name_of_Profile_here>
RetryFailedAuthentications = no
```
### Table 50: winauth.aut [WindowsDomain] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowExpiredPasswordsForUsers</td>
<td>A value of yes means that when the incoming username/password pair can be validated but the password has expired (under Domain User authentication), the server responds with an Access-Accept. A value of no means the server responds with an Access-Reject. If set to yes and you do not provide a ProfileForExpiredUsers value, the Access-Accept response contains the return list from the Domain User entry that matches the incoming username. This option is recommended for Domain Users. If set to yes and you provide a ProfileForExpiredUsers, the return list from that profile is used. Default value is no.</td>
</tr>
<tr>
<td>AllowExpiredPasswordsForGroups</td>
<td>If set to yes, the server responds with an Access-Accept when the incoming username/password pair can be validated but the password has expired (under Domain Group authentication). If set to no, the server responds with an Access-Reject. If set to yes and you provide a ProfileForExpiredGroups, the return list from that profile is used. This option is strongly recommended if you allow expired passwords for Domain Groups. If set to yes and you do not provide a ProfileForExpiredGroups value, the Access-Accept response contains the return list from the first Domain Group entry (alphabetically) in the server database. Default value is no.</td>
</tr>
<tr>
<td>AllowMachineLogin</td>
<td>Machine authentication is useful for sites that want a host on the network even when a user is not logged in. When machine authentication is enabled, a host’s Windows domain credentials (certificate or domain password) are used to connect the host to the network. If set to yes, machine authentication is enabled. If set to no, machine authentication is disabled. Default value is yes. <strong>NOTE:</strong> You must enter 1 for the First-Handle-Via-Auto-EAP setting in the [Windows Domain User] and [Windows Domain Group] sections of eap.ini if you want to use machine authentication. For more information, see “eap.ini File” on page 184.</td>
</tr>
<tr>
<td>ProfileForExpiredUsers</td>
<td>Names a profile entry in the Steel-Belted Radius database. This entry provides the return list for responses for all users who are accepted by the server under Domain User “expired password” conditions.</td>
</tr>
<tr>
<td>ProfileForExpiredUsersInGroups</td>
<td>Names a profile entry in the Steel-Belted Radius database. This entry provides the return list for responses for all users who are accepted by the server under Domain Group “expired password” conditions. This option is strongly recommended for Domain Groups.</td>
</tr>
</tbody>
</table>
Table 50: winauth.aut [WindowsDomain] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| PrequalifyCheckList   | ■ If set to yes, Steel-Belted Radius performs checklist processing on each domain object in the database before trying to authenticate a user request. If checklist processing fails, the object is skipped.  
|                       | ■ If set to no, prequalification checklist processing is not performed.   |
|                       | Default value is no.                                                     |
| RetryFailedAuthentications | ■ If set to yes, Steel-Belted Radius attempts to authenticate a user after an authentication failure.  
|                        | ■ If set to no, Steel-Belted Radius does not attempt to reauthenticate a user after an authentication failure. |
|                       | Default value is no.                                                     |
Chapter 4
Attribute Processing Files

This chapter describes the usage and settings for the Steel-Belted Radius attribute processing and dictionary files, which specify RADIUS attributes.

Overview

For each product listed in the vendor.ini file, Steel-Belted Radius provides a dictionary (.dct) file. Dictionary files enable Steel-Belted Radius to exchange attributes with RADIUS clients. Like initialization files, dictionary files are loaded at startup time, and reside in the Steel-Belted Radius directory:

* .dct
dictionary.dcm

- Dictionary files identify the attributes Steel-Belted Radius should expect when receiving RADIUS requests from a specific type of device.
- Dictionary files identify the attributes Steel-Belted Radius should include when sending a RADIUS response to a specific type of device.

Figure 1 illustrates the format of a dictionary file.
Figure 1: Sample Dictionary File

#########################################################################
# Juniper.dct - RADIUS dictionary for Juniper M-160 and M-40Es
# (See README.DCT for more details on the format of this file)
#########################################################################
# Use the RADIUS specification attributes
#
@radius.dct
#
# Juniper specific parameters
#
MACRO Juniper-VSA(t,s) 26 [vid=2636 type1=%t% len1=+2 data=%s%]

ATTRIBUTE Juniper-Local-User-Name Juniper-VSA(1, string) r
ATTRIBUTE Juniper-Allow-Commands Juniper-VSA(2, string) r
ATTRIBUTE Juniper-Deny-Commands Juniper-VSA(3, string) r
ATTRIBUTE Juniper-Allow-Configuration Juniper-VSA(4, string) r
ATTRIBUTE Juniper-Deny-Configuration Juniper-VSA(5, string) r

#########################################################################
# Juniper.dct - Juniper Networks dictionary
#########################################################################

Dictionary File Location

Windows: Dictionary files must be placed in the same directory as the Steel-Belted Radius service. While starting up, Steel-Belted Radius scans its home directory for all files with an extension of .dct (standard dictionary files) and uses the list to create a “master” dictionary, which includes all known attributes.

Solaris/Linux: Dictionary files must be placed in the same directory as the Steel-Belted Radius daemon. During initialization, Steel-Belted Radius reads the file dictionary.dcm in the server directory to get a list of files with an extension of .dct (standard dictionary files) and uses the list to create a “master” dictionary, which includes all known attributes.

Dictionary File Records

Records in a dictionary file must begin with one of the keywords listed in Table 51.

Table 51: Dictionary File Keywords

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>@</td>
<td>Include the referenced file</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>Define a new attribute</td>
</tr>
<tr>
<td>VALUE</td>
<td>Define a named integer value for an attribute</td>
</tr>
<tr>
<td>MACRO</td>
<td>Define a macro used to simplify repetitive definitions</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>Define options beyond the scope of attribute definitions</td>
</tr>
<tr>
<td>#</td>
<td>Ignore this text (comment)</td>
</tr>
</tbody>
</table>
Chapter 4: Attribute Processing Files

Editing Dictionary Files

The product-specific files shipped with Steel-Belted Radius reflect specific vendors’ implementations of RADIUS clients. Therefore, you do not usually need to modify the dictionary files shipped with Steel-Belted Radius. However, if your network access device vendor provides information about a new product, a new attribute, or a new value for an attribute, you can add this information to your existing Steel-Belted Radius configuration by editing dictionary files.

Before you edit an existing dictionary file or create a new one, you must do the following to integrate your changes into Steel-Belted Radius:

1. Add a new vendor-product entry to vendor.ini so that you can reference the new dictionary while configuring Steel-Belted Radius.
2. Place your dictionary file in the same directory as the Steel-Belted Radius service or daemon.
3. Edit the dictiona.dcm file so that it includes your new dictionary file.
4. Stop and restart the server.

Include Records

Records in a dictionary file that begin with the @ character are treated as special include records. The string that follows the @ character identifies the name of a dictionary file whose contents are to be included. For example, the entry @vendorA.dct would include all of the entries in the file vendorA.dct.

Include records are honored only one level deep. For example, if file vendorA.dct includes file radbase.dct and radbase.dct includes radacct.dct, vendorA.dct incorporates records in radbase.dct but not those in radacct.dct.

Master Dictionary File

The master dictionary dictiona.dcm consists of include records that reference vendor-specific dictionaries. The order in which vendor-specific dictionaries are included in the master dictionary has significance only if two vendor-specific dictionaries contain conflicting definitions for the same attribute or attribute value. The first definition of an attribute or attribute value takes precedence over later definitions of the same attribute or attribute value. For example, if master dictionary dictiona.dcm consists of the following include records:

@vendorA.dct
@vendorB.dct
@vendorC.dct

then attributes and attribute values defined in vendorA.dct override attributes and attribute values defined in vendorB.dct or vendorC.dct, and attributes and attribute values in vendorB.dct override attributes and values defined in vendorC.dct.
ATTRIBUTE Records

Attribute records conform to the following syntax:

```
ATTRIBUTE attrib_name attrib_id syntax_type flags
```

**Table 52: ATTRIBUTE Record Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>attrib_name</td>
<td>Name of the attribute (up to 31 characters with no embedded blanks).</td>
</tr>
<tr>
<td>attrib_id</td>
<td>Integer in the range 0 to 255 identifying the attribute's encoded RADIUS identifier.</td>
</tr>
<tr>
<td>syntax_type</td>
<td>Syntax type of the attribute.</td>
</tr>
<tr>
<td>flags</td>
<td>Defines whether an attribute appears in the checklist, the return list (or both), whether it is multi-valued and whether it is orderable.</td>
</tr>
</tbody>
</table>

**NOTE:** One limitation of standard dictionary files (the `attrib_id` of all the attribute records must be unique) is waived for the master dictionary file. Multiple vendors can define different attribute names for the same attribute identifier (assuming the attribute identifier is not already used in the base RADIUS specification). Since attributes in the Steel-Belted Radius database are stored by name (rather than by `attrib_id`), this introduces no ambiguity into the database.

The following example illustrates a typical attribute record:

```
ATTRIBUTE Framed-IP-Netmask 9 ipaddr Cr
```

This attribute record specifies all of the following:

- An attribute named `Framed-IP-Netmask` is supported.
- The attribute’s encoded RADIUS identifier is 9.
- The attribute must use the syntax of an IP address.
- Flag characters specify that the attribute can appear multiple times in a checklist (C) and at most one time in a return list for User or profile entries (r) in the Steel-Belted Radius database.

**Attribute Name and Identifier**

No two attribute records in a single dictionary file should have the same `attrib_name` or `attrib_id`. If a duplicate `attrib_name` or `attrib_id` is encountered, the later definition of the attribute is ignored in favor of the earlier one.

**Syntax Type Identifier**

Standard `syntax_type` identifiers are listed in Table 53.
Chapter 4: Attribute Processing Files

### Compound Syntax Types

In addition to the standard `syntax_type` identifiers listed in Table 53, the dictionary can accommodate compound syntax types for use in defining vendor-specific attributes. Instead of a single `syntax_type` identifier, one or more of the options listed in Table 54 can be combined inside square brackets to form a compound syntax type.

#### Table 53: Syntax Type Identifiers

<table>
<thead>
<tr>
<th>Syntax Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>hexadecimal</td>
<td>Hexadecimal string</td>
</tr>
<tr>
<td>hex4</td>
<td>4-byte (32-bit) unsigned hexadecimal number.</td>
</tr>
<tr>
<td>int1</td>
<td>1-byte (8-bit) unsigned decimal number.</td>
</tr>
<tr>
<td>int4, integer</td>
<td>4-byte (32-bit) unsigned decimal number.</td>
</tr>
<tr>
<td>signed-integer</td>
<td>4-byte (32-bit) signed decimal number. A number with a 1 in the first bit position is interpreted as a negative number.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>IP address or IP netmask attribute.</td>
</tr>
<tr>
<td>ipaddr-pool</td>
<td>IPv4 address selected from an IP address pool.</td>
</tr>
<tr>
<td>ipxaddr-pool</td>
<td>IPX network number selected from an IPX address pool.</td>
</tr>
<tr>
<td>string</td>
<td>String attribute (includes null terminator).</td>
</tr>
<tr>
<td>stringnz</td>
<td>String attribute (without null terminator).</td>
</tr>
<tr>
<td>time</td>
<td>Time attribute (number of seconds since 00:00:00 GMT, 1/1/1970).</td>
</tr>
</tbody>
</table>

**NOTE:** Signed integer support is limited to attributes received in packets and processing relating to those attributes, such as accounting logs, authentication logs, authentication reports, and SQL plug-ins. SBR Administrator does not support signed integers, and treats signed and unsigned integers as unsigned integers.

#### Table 54: Compound Syntax Types

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vid = nnn</code></td>
<td>The device manufacturer’s SMI Network Management Private Enterprise code (assigned by ISO) in decimal form.</td>
</tr>
<tr>
<td><code>typeN = nnn</code></td>
<td>Type setting for vendor-specific attribute as defined in the RADIUS specification; N specifies the length of the field (in bytes), nnn specifies the decimal value of the field.</td>
</tr>
<tr>
<td><code>lenN = nnn</code></td>
<td>Length field for vendor-specific attribute as defined in the RADIUS specification; N specifies the length of the field (in bytes), nnn specifies the decimal value of the field (a plus sign prior to the value indicates that the length of the data portion is to be added to nnn to obtain the actual length).</td>
</tr>
</tbody>
</table>
An example of a vendor-specific attribute definition follows:

**ATTRIBUTE vsa-xxx 26 [vid=1234 type1=1 len1=+2 data=string] R**

**Flag Characters**
The flags setting consists of the concatenation of one or more flag characters from the list in Table 55.

**Table 55: Flag Characters**

<table>
<thead>
<tr>
<th>Flag Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>b or B</td>
<td>Indicates that an attribute may be bundled in a single Vendor-Specific-Attribute for a particular vendor id. It may be included as one of a series of subattributes within a single VSA.</td>
</tr>
<tr>
<td>c</td>
<td>Attribute can appear once within a user or profile check-list.</td>
</tr>
<tr>
<td>C</td>
<td>Attribute can appear multiple times within a user or profile check-list.</td>
</tr>
<tr>
<td>r</td>
<td>Attribute can appear once within a user or profile return-list.</td>
</tr>
<tr>
<td>R</td>
<td>Attribute can appear multiple times within a user or profile return-list.</td>
</tr>
<tr>
<td>t</td>
<td>Attribute can appear once within a tunnel attribute list.</td>
</tr>
<tr>
<td>T</td>
<td>Attribute can appear multiple times within a tunnel attribute list.</td>
</tr>
<tr>
<td>o or O</td>
<td>Attribute is orderable; the administrator can control the order in which such attributes are stored in the Steel-Belted Radius database (this flag makes sense only for multi-valued attributes).</td>
</tr>
</tbody>
</table>

**VALUE Records**
Value records are used to define names for specific integer values of previously defined integer attributes. Value records are never required, but are appropriate where specific meaning can be attached to an integer value of an attribute. The value record must conform to the following syntax:

**VALUE attrib_name value_name integer_value**
Chapter 4: Attribute Processing Files

No two value records in a dictionary file should have the same `attrib_name` and `value_name` or the same `attrib_name` and `integer_value`. If a duplicate is encountered, the later definition of the attribute value is ignored in favor of the earlier one (the earlier one is considered to be an override).

The following example illustrates the use of the VALUE record to define more user-friendly attribute values for the Framed-Protocol attribute:

```
ATTRIBUTE Framed-Protocol     7     integer     Cr
VALUE      Framed-Protocol     PPP           1
VALUE      Framed-Protocol     SLIP          2
```

Using these dictionary records, the administrator need not remember that the integer value 1 means PPP and the integer value 2 means SLIP when used in conjunction with the Framed-Protocol attribute. Instead, the Steel-Belted Radius Administrator program lets you choose from a list of attribute values including PPP and SLIP.

**Macro Records**

Macro records are used to streamline the creation of multiple vendor-specific attributes that include many common parameters. A macro record can be used to encapsulate the common parts of the record. The macro record must conform to the following syntax:

```
MACRO macro_name(macro_vars) subst_string
```

The following example illustrates the use of a macro that simplifies the specification of multiple vendor-specific attributes:

```
MACRO Cisco-VSA(t, s) 26 [vid=9 type1=%t% len1=+2 data=%s%]
ATTRIBUTE   Cisco-xxx   Cisco-VSA(1, string)    R
ATTRIBUTE   Cisco-yyyy   Cisco-VSA(4, int4)     C
ATTRIBUTE   Cisco-zzz    Cisco-VSA(9, ipaddr)   r
```
The macro preprocessor built into the Steel-Belted Radius dictionary processing would translate the records in the preceding example to the following records before being processed.

```
ATTRIBUTE Cisco-xxx 26 [vid=9 type1=1 len1=+2 data=string] R
ATTRIBUTE Cisco-yyy 26 [vid=9 type1=4 len1=+2 data=int4] C
ATTRIBUTE Cisco-zzz 26 [vid=9 type1=9 len1=+2 data=ipaddr] r
```

**OPTION Records**

By default, each vendor-specific attribute is encoded in a single VSA attribute. The format of a VSA attribute is described in Table 58.

**Table 58: OPTION Records**

<table>
<thead>
<tr>
<th>Bits</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 7</td>
<td>Type: contains the value 26</td>
</tr>
<tr>
<td>8 - 16</td>
<td>Length of data in bytes</td>
</tr>
<tr>
<td>17 - 47</td>
<td>Vendor ID</td>
</tr>
<tr>
<td>48 - on</td>
<td>Vendor data</td>
</tr>
</tbody>
</table>

If you provide a parameter to the OPTION setting, however, multiple vendor-specific attributes can be present in the vendor-data portion of a single VSA record.

The OPTION record must conform to the following format:

```
OPTION bundle-vendor-id = vid
```

**NOTE:** You must set the B flag for attribute bundling to occur. For a particular vendor-specific attribute to be bundled, you must set the OPTION record for the vendor’s vendor-ID and set the B (or b) flag for the specific attribute.

The Nortel Rapport dictionary supports this option, for example. If you want to combine Nortel’s vendor-specific attributes in a single VSA, you would provide the entry:

```
OPTION bundle-vendor-id=562
```

This is because 562 is Nortel’s Vendor ID, as set in the MACRO record. The Nortel Rapport vendor-specific attributes now would be concatenated within the vendor-data portion of a RADIUS VSA attribute (up to 249 octets).
classmap.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE
**Not Used By:** —

The classmap.ini initialization file specifies what Steel-Belted Radius does with RADIUS attributes encoded in one or more Class attributes included in accounting requests it receives.

**[AttributeName] Section**

The [AttributeName] section of classmap.ini specifies whether RADIUS information encapsulated in a Class attribute should be appended to an accounting request or replace a current value in an accounting request. If one attribute is replaced by another, the original attribute can be added to the request with a different identifier.

```
[AttributeName]
<add | replace> = Attribute [,Attribute]
```

**Table 59: classmap.ini [Attributename] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttributeName</td>
<td>Name of the attribute encoded into the Class attribute by the authenticating server.</td>
</tr>
<tr>
<td>&lt;add</td>
<td>replace&gt;</td>
</tr>
<tr>
<td>Attribute</td>
<td>Specifies the name of the attribute that should be added to the accounting request, which contains the original value of the attribute identified by AttributeName.</td>
</tr>
<tr>
<td>[,Attribute]</td>
<td>Specifies the name of the attribute in the accounting request that should contain the value of the attribute displaced when the value of AttributeName replaces the existing Attribute value. Valid only when the replace keyword is used.</td>
</tr>
</tbody>
</table>

**NOTE:** The RADIUS Class attribute cannot contain IPv6 attributes.

In the following example, the encapsulated **User-Name** attribute would replace the existing **User-Name** in the accounting request.

```
[User-name]
replace = User-Name
```
In the following example, the encapsulated User-Name attribute would be placed in the accounting request as User-Name, and the original value for User-Name would be added to the request as Funk-Full-User-Name.

[User-name]
replace = User-Name, Funk-Full-User-Name

In the following example, the encapsulated User-Name attribute would be added to the accounting request as a new attribute, and the original User-Name attribute would remain unchanged.

[User-Name]
add = Funk-Full-User-Name
filter.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not used by:** —

You should use the SBR Administrator to maintain settings in the filter.ini file. You should not edit the filter.ini file manually.

The filter.ini configuration file lets you set up rules for filtering attributes into and out of RADIUS packets.

**Filter Rules**

Each filter in the filter.ini file consists of the filter name in square brackets ([name]) followed by the rules for that filter.

Each rule takes one of the following three forms:

`keyword attribute value`  
`keyword attribute`  
`keyword`

Table 60 lists valid syntax combinations.

<table>
<thead>
<tr>
<th>filter.ini Rule Syntax</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLOW</td>
<td>This keyword by itself specifies that all attributes, regardless of value, are to be allowed in the packet.</td>
</tr>
<tr>
<td>ALLOW attribute</td>
<td>This rule specifies that this attribute is allowed in the packet, regardless of its value.</td>
</tr>
<tr>
<td>ALLOW attribute value</td>
<td>The rule lists a specific attribute/value pair to allow in the packet.</td>
</tr>
</tbody>
</table>
| EXCLUDE                | The keyword by itself specifies that all attributes, regardless of value, are to be excluded from the packet.  
                         | EXCLUDE is the default action for a filter. |
| EXCLUDE attribute      | The rule specifies that this attribute is excluded from the packet, regardless of its value. |
| EXCLUDE attribute value| The rule specifies an attribute/value pair to exclude from the packet. |
| ADD attribute value    | The rule lists a specific attribute/value pair to add to the packet. The attribute is added after all other rules are processed. |
| REPLACE attr1 WITH attr2 | The rule specifies that any occurrence of attr1 are replaced by attr2, which retains attr1’s value. |
| REPLACE attr1 WITH attr2 v2 | The rule specifies that any occurrence of attr1 (regardless of value) is replaced by attr2 whose value is set to v2. |
An attribute is **ADD**ed to a packet only if it is legal to do so. Some attributes can appear only once in a RADIUS packet; others can appear multiple times. If an attribute that is the subject of an **ADD** rule is already present in the packet (after processing **ALLOW** and **EXCLUDE** rules) and the attribute can only appear once, the **ADD** rule is not processed and the second instance of the attribute is not added.

The Steel-Belted Radius dictionary file `radius.dct` provides string aliases for certain integer values defined in the RADIUS standard. You can use these strings in attribute filter rules.

### Order of Filter Rules

The order of rules is important. General default rules that take no parameters, such as **ALLOW** (allow all attributes unless otherwise specified) or **EXCLUDE** (exclude all attributes unless otherwise specified) must appear as the first rule in the filter. Later rules supersede earlier rules; the last applicable rule “wins.” **ADD** and **REPLACE** rules are applied after the **ALLOW** and **EXCLUDE** rules.

More specific rules with more parameters (**ADD** `attribute` `value`) act as exceptions to less specific rules with fewer parameters (**ALLOW** `attribute`, **EXCLUDE**). For example, you might want to **ALLOW** a certain attribute and **EXCLUDE** one or more specific values for that attribute. Or you might **EXCLUDE** all attributes, **ALLOW** specific attributes, and **ADD** specific attribute/value pairs.

You can use two basic approaches to designing a filter:

- **Start the rule list with a default **EXCLUDE** rule (no parameters) and add **ALLOW** rules for any attributes or attribute/value pairs that you want to insert into the packet. **ADD** and **REPLACE** rules may be used.**

- **Start the rule list with a default **ALLOW** rule (no parameters) and add **EXCLUDE** rules for any attributes or attribute/value pairs that you want to remove from the packet. **ADD** and **REPLACE** rules may be used.**

The default action for `filter.ini` is **EXCLUDE**. If a filter does not contain any rules, the filter removes all attributes from a packet when the filter is applied.

<table>
<thead>
<tr>
<th><code>filter.ini</code> Rule Syntax</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>REPLACE attr1 v1 WITH attr2</code></td>
<td>The rule specifies that any occurrence of <code>attr1</code> whose value is <code>v1</code> is replaced by <code>attr2</code> (which keeps value <code>v1</code>).</td>
</tr>
<tr>
<td><code>REPLACE attr1 v1 WITH attr2 v2</code></td>
<td>The rule specifies that any occurrence of <code>attr1</code> whose value is <code>v1</code> is replaced by <code>attr2</code> having a value <code>v2</code>.</td>
</tr>
</tbody>
</table>
Values in Filter Rules

The value of an attribute is interpreted based on the type of the attribute in its attribute dictionary. Table 61 lists the meaning of each attribute type.

Table 61: Filter Rule Values

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>hexadecimal</td>
<td>A hexadecimal value is specified as a string. Special characters may be included using escape codes.</td>
</tr>
<tr>
<td>int1, int4, integer</td>
<td>1- or 4-byte unsigned decimal number (integer is equivalent to int4).</td>
</tr>
<tr>
<td>NOTE: The Steel-Belted Radius dictionary file radius.dct provides string aliases for certain integer values defined in the RADIUS standard. You can use these strings in attribute filter rules.</td>
<td></td>
</tr>
<tr>
<td>ipaddr, ipaddr-pool</td>
<td>An IP address in dotted notation; for example:</td>
</tr>
<tr>
<td></td>
<td>EXCLUDE NAS-IP-Address 127.0.0.1</td>
</tr>
<tr>
<td>ipxaddr-pool</td>
<td>A sequence of hex digits; for example:</td>
</tr>
<tr>
<td></td>
<td>ALLOW Framed-IPX-Network 0042A36B</td>
</tr>
<tr>
<td>string</td>
<td>A string attribute (includes null terminator). A string is specified as text. The text may be enclosed in double-quotes (&quot;). The text is interpreted as a regular expression. Backslash () is the escape character. Escape codes are interpreted as follows:</td>
</tr>
<tr>
<td>Code</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>\a</td>
<td>7</td>
</tr>
<tr>
<td>\b</td>
<td>8</td>
</tr>
<tr>
<td>\f</td>
<td>12</td>
</tr>
<tr>
<td>\n</td>
<td>10</td>
</tr>
<tr>
<td>\r</td>
<td>13</td>
</tr>
<tr>
<td>\t</td>
<td>9</td>
</tr>
<tr>
<td>\v</td>
<td>11</td>
</tr>
<tr>
<td>\mm</td>
<td>\nn is a decimal value between 0 and 255</td>
</tr>
<tr>
<td>\xm</td>
<td>\nnm is a hexadecimal value between 00 and FF</td>
</tr>
<tr>
<td>\c</td>
<td>c is a single character, interpreted literally</td>
</tr>
<tr>
<td>Literal backslashes () within a string and double-quotes (&quot;) within quoted strings should be prefixed with an escape character. For example:</td>
<td></td>
</tr>
<tr>
<td>ADD Reply-Message Session limit is one hour</td>
<td></td>
</tr>
<tr>
<td>ADD Reply-Message &quot;Session limit is one hour&quot;</td>
<td></td>
</tr>
<tr>
<td>ADD Reply-Message &quot;Your user name is &quot;George&quot;&quot;</td>
<td></td>
</tr>
</tbody>
</table>
Referencing Attribute Filters

Steel-Belted Radius attribute filtering provides flexibility in packet processing. You can use the same filter for all packets in all realms. You can apply filtering to some realms, and not others. (To disable filtering for a realm, omit filtering parameters from the *.pro, *.dir, peapauth.aut, or ttlsauth.aut file.) Filtering is often used only for packets that are routed “out” to realms (the FilterOut parameter).

To reference the filtering rules defined in the filter.ini file in proxy or directed realm configurations, you must use the FilterOut and FilterIn parameters in the [Auth] and [Acct] sections of a RADIUS realm configuration file.

The full syntax used is:

```
[Auth]
FilterIn=name1
FilterOut=name2

[Acct]
FilterIn=name3
FilterOut=name4
```

where `name1`, `name2`, and so forth provide the names of filters, sections in the filter.ini file called `[name1]`, `[name2]`, and so forth. The `name` values in this syntax are completely independent of each other. They may be all the same, all different, or some combination of same and different.

When using the FilterIn and FilterOut parameters in the [Auth] and [Acct] sections, be sure to use the filter name without the square brackets (“name”, not “[name]”).

NOTE: If a [name] section is not found in the filter.ini file, it is equivalent to assigning a filter that EXCLUDEs all attributes. In other words, assigning a filter name that cannot be found causes the final packet to be emptied of all attributes.
NOTE: Do not allocate IP addresses from Steel-Belted Radius IP address pools in accounting filters. These addresses will be allocated but never released.
Attribute value pools allow Steel-Belted Radius to assign and return attribute sets dynamically when an Authorization Request is processed. This functionality is supported by the use of a vendor-specific attribute (VSA) called Funk-Round-Robin-Group. The value for this attribute is a string, and should be set to the name of a .rr suffix file that defines an attribute value pool. This value can therefore be set for a user or profile by using the SBR Administrator or the LDAP Configuration Interface (LCI), or by any other return list mechanism (such as database retrieval).

Attribute value pooling allows for a dynamic allocation of attribute values sets, so that attributes needed to configure changeable and complex situations do not have to be assigned in static profiles. This functionality is supported by the use of a vendor-specific attribute called Funk-Round-Robin-Group. The value for this attribute is a string, and should be set to the name of a .rr suffix file that defines an attribute value pool.

A .rr file is defined as follows:

```
[Sets]
SetName1 = Weight1
SetName2 = Weight2
...
[SetName1]
AttributeName1.1 = AttributeValue1.1
AttributeName1.2 = AttributeValue1.2
...
```

Steel-Belted Radius maintains “round-robin” statistics for each attribute value pool so that weight calculations can be performed properly. When a user who belongs to a profile that has been assigned to a particular attribute value pool logs in, the round-robin values are incremented to determine which Attribute Value set should be assigned to the user. This attribute set is added to the return list of the Access-Accept.

Attribute value pooling can be used in several ways. For example, the Acme Company wants off-site employees to be able to establish tunnels to the company network. The Acme Company maintains three tunnel connection endpoints to which end users can create VPNs into the corporate network, each of these with different capacities. The company would define an attribute value pool of three attribute sets, each describing how to establish a tunnel with one of these connection points. These attribute sets should be weighted according to the capacity of the three connection points. Figure 2 illustrates a sample acme.rr file.
Chapter 4: Attribute Processing Files

Figure 2: Sample *.rr file (acme.rr)

;acme.rr
[Sets]
VPN1=20
VPN2=12
VPN3=7

[VPN1]
Tunnel-Server-Endpoint = 8.4.2.1
Tunnel-Password = GoodGuess

[VPN2]
Tunnel-Server-Endpoint = 8.4.2.2
Tunnel-Password = BestGuess

[VPN3]
Tunnel-Server-Endpoint = 8.4.2.4
Tunnel-Password = OurSecret

To make this attribute value pool visible, the Acme Company would define a Funk-Round-Robin-Group VSA and assign it to the users (or the profile assigned to these users) and make the value of the VSA point to the acme.rr file shown in Figure 2.

Funk-Round-Robin-Group = acme.rr

Refer to the Steel-Belted Radius Administration Guide for more information on using attribute value pooling.
spi.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE
**Not Used By:** —

The spi.ini initialization file defines encryption keys and identifies the servers from which Steel-Belted Radius processes encrypted Class attributes in accounting requests. The spi.ini file allows one Steel-Belted Radius server to decode accounting requests for sessions that were authenticated on a different Steel-Belted Radius server. Class attributes received from servers not specified in spi.ini are ignored.

All Steel-Belted Radius servers that may receive authentication and accounting requests from a common network access device must be configured with similar spi.ini files, which must list the IP addresses of all the servers in that “cluster.” This allows one server to authenticate a user and generate an encrypted Class attribute that can be decrypted and processed by any other server in the cluster.

**[Keys] Section**

The [Keys] section of spi.ini specifies the list of encryption keys used to encode subattributes encapsulated within Class attributes.

```ini
[Keys]
CurrentKey = n
1 = value
2 = value
```

**Table 62: spi.ini [Keys] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| CurrentKey | Specifies the encryption key that is currently active, where \( n \) is 0 or the number of a key listed in the [Keys] section:  
  \[ 0 – Generate and use a unique random key to encrypt Class attributes. Used only when the Steel-Belted Radius server does not exchange encrypted Class attributes with other servers. \]  
  \[ n – Use the specified key to encrypt Class attributes. \]  
  Default value is 0. |

\( n = value \) | Specifies the number and value of the encryption key. |

In the following example, the Steel-Belted Radius server generates a unique random key to encrypt Class attributes.

```
[Keys]
CurrentKey = 0
```

In the following example, the second key (swordfish) is currently active and used to encrypt Class attributes. The other keys in this section can be used to decrypt Class attributes received from other servers in the same cluster.
[Keys]
CurrentKey = 2
1 = firstkey
2 = swordfish
3 = mypassword

[Hosts] Section

The [Hosts] section of spi.ini identifies the IP address of servers from which received Class attributes are parsed for encapsulated/encrypted subattributes. Class attributes from servers not identified in the [Hosts] section of spi.ini are passed without special processing.

The information in the [Hosts] section is used to compute the server’s identifier, which is included in the Class attribute. If one of a host’s interfaces is included in the [Hosts] section, that interface is used to compute the server identifier. If more than one interface for a host is listed, the IP address of the last interface listed is used. If no matching address is found, the host’s primary IP address is used. Addresses not corresponding to a host interface are used to configure the collection of other servers whose Class attributes are accepted.

In the following example, three servers are identified as belonging to a cluster.

[Hosts]
192.168.15.21
192.168.23.121
192.168.23.205
vendor.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE  
**Not Used By:** —

The vendor.ini initialization file contains information that allows Steel-Belted Radius to work with the products of other vendors.

**[Vendor-Product Identification] Section**

The [Vendor-Product Identification] section of vendor.ini (Table 63) identifies and provides information about the network access devices that can be used with Steel-Belted Radius.

**Table 63: vendor.ini [Vendor-Product Identification] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>vendor-product</td>
<td>Specifies the name of the product. A product name must be unique, cannot include blanks and must consist of 31 or fewer characters. These product names are used only in the Make/model list in the RADIUS Clients panel. This list is used when adding a new RADIUS client or when selecting a vendor-specific attribute.</td>
</tr>
<tr>
<td>dictionary</td>
<td>Specifies the dictionary file to use for this product. The dictionary file must be located in the same directory as the Steel-Belted Radius daemon or service. You do not need to specify an extension on the dictionary name; Steel-Belted Radius automatically attaches an extension of .DCT to the dictionary names listed in this parameter.</td>
</tr>
<tr>
<td>call-filter-attribute</td>
<td>Specifies the attribute used for call filter functions. Used only by Ascend/Lucent network access devices.</td>
</tr>
<tr>
<td>challenge-response-attribute</td>
<td>Specifies the attribute number in which a network access device sends responses to challenge sequences. If not specified, the default behavior is to expect responses to be encoded in the User-Password attribute.</td>
</tr>
<tr>
<td>data-filter-attribute</td>
<td>Specifies the attribute used for data filter functionality. Used only by Ascend/Lucent network access devices.</td>
</tr>
<tr>
<td>discard-after</td>
<td>Used for inbound proxy RADIUS servers that send username information in a “decorated” format. For example, if a proxy RADIUS server sends usernames of the form <strong>username@company,</strong> then specifying @ results in the @ delimiter character and all text after the @ delimiter character being discarded for authentication purposes, the string <strong>username</strong> is used.</td>
</tr>
<tr>
<td>discard-before</td>
<td>Used for inbound proxy RADIUS servers that send username information in a “decorated” format. For example, if a proxy RADIUS server sends usernames of the form <strong>company$Username,</strong> then specifying $ results in the $ delimiter character and all text before the $ delimiter character being discarded for authentication purposes, the string <strong>username</strong> is used.</td>
</tr>
<tr>
<td>help-id</td>
<td>Help context for the vendor’s product in the vendor information help file.</td>
</tr>
</tbody>
</table>
Vendor.ini File

Chapter 4: Attribute Processing Files

ignore-acct-ss
If set to Yes, the digital signature of accounting packets based on the shared secret is ignored. This accommodates devices that do not properly sign accounting packages.
Default value is No.

ignore-ports
Determines whether Steel-Belted Radius may infer that one user has logged off if the port that was assigned to that user is now being used by another user.
- If set to No, an inference is made and the previous user is removed from the Active Users list.
- If set to Yes, no inference is made and both users are deemed active.
Default value is No.

max-eap-fragment
Specifies a maximum EAP fragment length on a make/model basis. The maximum EAP fragment length emitted by TLS or TTLS is the lesser of the maximum specified in their .eap.aut files and this setting.
Default value is 1020. This may be inefficient, however, as the fragment length must be set to a number low enough to work with all of a customer’s Access Points.

port-number-usage
- If set to per-port-type, entries in the Active List containing duplicate port numbers and port types are deleted.
- If set to unique, entries in the Active List containing duplicate port numbers are deleted; port type information is ignored.
Default value is per-port-type.

product-scan-acct
Specifies the name of the section in the vendor.ini file that contains rules for dynamically determining the product associated with an accounting request by the contents of the request packet.

product-scan-auth
Specifies the name of the section in the vendor.ini file that contains rules for dynamically determining the product associated with an authentication request by the contents of the request packet.

send-class-attribute
If set to No, the Class attribute is not sent to the client on Access-Accept. (This feature is designed to accommodate devices that don’t handle the Class attribute properly.)
Default value is Yes.

send-session-timeout-on-challenge
- If set to Yes, the Session-Timeout attribute is sent to the client on Access-Challenge responses that include EAP messages. This attribute advises a network access device on how long it should wait for a user response to the challenge.
- If set to No, the Session-Timeout attribute is not sent to the client on Access-Challenge responses that include EAP messages.
Default value is Yes.

Table 63: vendor.ini [Vendor-Product Identification] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ignore-acct-ss</td>
<td>If set to Yes, the digital signature of accounting packets based on the shared secret is ignored. This accommodates devices that do not properly sign accounting packages. Default value is No.</td>
</tr>
</tbody>
</table>
| ignore-ports     | Determines whether Steel-Belted Radius may infer that one user has logged off if the port that was assigned to that user is now being used by another user. 
- If set to No, an inference is made and the previous user is removed from the Active Users list.
- If set to Yes, no inference is made and both users are deemed active. Default value is No. |
| max-eap-fragment | Specifies a maximum EAP fragment length on a make/model basis. The maximum EAP fragment length emitted by TLS or TTLS is the lesser of the maximum specified in their .eap.aut files and this setting. Default value is 1020. This may be inefficient, however, as the fragment length must be set to a number low enough to work with all of a customer’s Access Points. |
| port-number-usage| If set to per-port-type, entries in the Active List containing duplicate port numbers and port types are deleted. 
- If set to unique, entries in the Active List containing duplicate port numbers are deleted; port type information is ignored. Default value is per-port-type. |
| product-scan-acct| Specifies the name of the section in the vendor.ini file that contains rules for dynamically determining the product associated with an accounting request by the contents of the request packet. |
| product-scan-auth| Specifies the name of the section in the vendor.ini file that contains rules for dynamically determining the product associated with an authentication request by the contents of the request packet. |
| send-class-attribute| If set to No, the Class attribute is not sent to the client on Access-Accept. (This feature is designed to accommodate devices that don’t handle the Class attribute properly.) Default value is Yes. |
| send-session-timeout-on-challenge| If set to Yes, the Session-Timeout attribute is sent to the client on Access-Challenge responses that include EAP messages. This attribute advises a network access device on how long it should wait for a user response to the challenge. 
- If set to No, the Session-Timeout attribute is not sent to the client on Access-Challenge responses that include EAP messages. Default value is Yes. |
Product-Scan Settings

Used by: GEE, SPE, SPE + MIM, SPE + EAP
Not used by: EE

After you define a Vendor-Product entry in vendor.ini, the name of this entry can be selected in the RADIUS Clients window as a possible value for the Make/model field. The Product-Scan-Auth and Product-Scan-Acct settings can be used within a Vendor-Product entry to permit dynamic make/model selection to occur. These settings enable Steel-Belted Radius to examine the incoming packet to determine the make/model of the network access device that originated the packet.

A dynamic Vendor-Product entry might appear as follows:

Vendor-Product = DeviceNameInRASClientsList
Product-Scan-Auth = MakeModelSelect
Product-Scan-Acct = MakeModelForAccounting

[MakeModelForAuthentication]
Product = String
Product = String

[MakeModelForAccounting]
Product = String
Product = String

Table 64: vendor.ini Product-Scan Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor-Product</td>
<td>Creates a label that appears as a selection in the Make/Model list in the RADIUS Clients window of the SBR Administrator.</td>
</tr>
<tr>
<td>Product-Scan-Auth = name</td>
<td>Applies only to authentication servers. name references a section heading that appears elsewhere in vendor.ini.</td>
</tr>
<tr>
<td>Product-Scan-Acct = name</td>
<td>Applies only to accounting servers. name references a section heading that appears elsewhere in vendor.ini.</td>
</tr>
</tbody>
</table>
The following example would be appropriate in a configuration whose RASs were mostly Ascend devices:

Product-Scan-Auth = Bigco Special Scan

[Bigco Special Scan]
Ascend MAX Family = \x2c?
Nortel Versalar Remote Access Concentrator = \x1a?\x00\x00\x06\x30
US Robotics NETServer = \x1a?\x00\x00\x01\xad
Ascend MAX Family =

The preceding example sets up dynamic make/model selection for authentication and states that the identity of the client device should be determined by seeking matches in the following order:

1. Is the attribute with identifier number 0x2c (Acct-Session-Id), with a value of any length (indicated by the question mark character), found in the incoming authentication packet? If so, the originating network access device is a member of the Ascend MAX Family; use that vendor-specific dictionary.

2. Is the vendor-specific attribute with identifier number 0x1a (Vendor-Id), with a value of any length (indicated by the question mark character), present in the packet? If so, does it have the value 1584 (0x630) which indicates a Nortel Networks Versalar RAC? If so, use that vendor-specific dictionary (provided with Steel-Belted Radius).

3. Is the Vendor-Id attribute present, with any length, and if so, does it have the value 429 (0x1ad) which indicates a US Robotics NETServer? If so, use that vendor-specific dictionary (provided with Steel-Belted Radius).
4. If no match can be found using the rules specified in this section, then use the vendor-specific dictionary for the Ascend MAX Family.

NOTE: You should include a default entry in this section. When there is no default, if an Access-Request is received with no vendor-specific attributes of any kind, the user may be rejected due to invalid resources, as the RADIUS server cannot associate a valid dictionary with the request. Using the example:

- Standard RADIUS =

as the last line in this section is a safe configuration.
Chapter 5

Address Assignment Files

This chapter describes the usage and settings for the Steel-Belted Radius initialization (.ini) files that are used to enable, disable, and configure IP address assignment, which is available for the GEE and SPE versions of Steel-Belted Radius.

<table>
<thead>
<tr>
<th>File</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp.ini</td>
<td>134</td>
</tr>
<tr>
<td>pool.dhc Files</td>
<td>136</td>
</tr>
</tbody>
</table>
dhcp.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

The dhcp.ini configuration file configures DHCP address pools so that IPv4 addresses can be assigned from a backend DHCP server, rather than from a standard Steel-Belted Radius IP address pool.

**NOTE:** Steel-Belted Radius does not support DHCP allocation of IPv6 addresses.

### [Settings] Section

The [Settings] section of the dhcp.ini file (Table 65) controls DHCP address allocation.

#### Table 65: dhcp.ini [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable      | - If set to 1, DHCP address allocation is enabled.  
- If set to 0, DHCP address allocation is disabled.  
Default value is 0. |
| Attempts    | Specifies the number of times a DHCP DISCOVER or REQUEST message is sent if no response is received.  
Default value is 3. |
| AttemptTimeout | Specifies the waiting period, in seconds, for a response to a DISCOVER or REQUEST message, before resending the message.  
Default value is 5 seconds. |
| OverallTimeout | Specifies the number of seconds for acquiring an IP address before DHCP address assignment is presumed to have failed.  
This timeout applies only to the DISCOVER/REQUEST sequence used to acquire an address initially, not to address renewal or release.  
Default value is 15 seconds.  
**Note:** While the timeout for the individual DISCOVER and REQUEST transactions is specified by Attempts and AttemptTimeout, Overall Timeout specifies the timeout for the entire sequence. |
| htype       | Specifies the client hardware type (0–255).  
This parameter is typically omitted, because the value is generated automatically. |
| Hlent       | Specifies the length of the client hardware address (1–16).  
This parameter is typically omitted, because the value is generated automatically. |
| Chaddr-prefix | Specifies the string that identifies the initial bytes of the client hardware address (chaddr). This string can include escape codes, including \nnn for decimal values and \xnnn for hex values.  
This parameter is typically omitted, because the value is generated automatically. |
Table 65: dhcp.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerPort</td>
<td>Specifies the UDP port number on which the DHCP server(s) listen. This setting should be specified only for non-standard DHCP configurations. Default value is 67, which is the standard DHCP server port.</td>
</tr>
<tr>
<td>LocalPort</td>
<td>Specifies the UDP port number that Steel-Belted Radius, acting as a relay agent, uses during DHCP communication. This setting should be specified for only non-standard DHCP configurations. Default value is 67, which is the standard DHCP server port.</td>
</tr>
<tr>
<td>Pad</td>
<td>Specifies the minimum number of bytes for a DHCP request message. Messages smaller than this number are padded with 0s. Certain DHCP servers discard messages smaller than a certain value. This option allows interoperability with such servers. Default value is 300.</td>
</tr>
</tbody>
</table>

The following is a sample dhcp.ini file:

```
[Settings]
Enable = 1
Attempts = 3
AttemptTimeout = 2
OverallTimeout = 10
```

**[Pools] Section**

The [Pools] section lists all DHCP pool names (specified in the pool.dhc file, which is described on page 136) in the following format:

```
[Pools]
pool 1
pool 2
:
```

For example:

```
[Pools]
DHCP_SERVER1
DHCP_SERVER_SALES
```
**pool.dhc Files**

Each pool listed in the [Pools] section of the dhcp.ini file must be a corresponding pool.dhc file that configures that pool.

**[Settings] Section**

The [Settings] section of the pool.dhc file (Table 66) controls DHCP lease information.

### Table 66: pool.dhc [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LeaseTime</td>
<td>Set to the lease time, in seconds, to request from the DHCP server.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1 day.</td>
</tr>
<tr>
<td>MinLeaseTime</td>
<td>Set to the minimum lease time, in seconds. Offers from DHCP servers with</td>
</tr>
<tr>
<td></td>
<td>lease time less than this minimum are ignored.</td>
</tr>
<tr>
<td></td>
<td>Default value is the value set for LeaseTime.</td>
</tr>
<tr>
<td>TargetAddress</td>
<td>Set to the address to which DISCOVER messages are sent.</td>
</tr>
<tr>
<td></td>
<td>Default value is 255.255.255.255, the local broadcast address.</td>
</tr>
<tr>
<td></td>
<td>This entry should normally remain unchanged, to allow DHCP DISCOVER</td>
</tr>
<tr>
<td></td>
<td>messages to be broadcast.</td>
</tr>
</tbody>
</table>

**[Request] Section**

The [Request] section allows options in the DHCP DISCOVER and REQUEST messages to be constructed from attributes in the RADIUS Access-Request and from pre-configured literal values in the following way:

```plaintext
[Request]
DHCP option = RADIUS attribute or literal value
DHCP option = RADIUS attribute or literal value
```

The DHCP option contains of the following fields (brackets ([ ]) indicate optional text). Fields are not separated by spaces.

- [vendor-specific] option [offset] format

### Table 67: pool.dhc [Request] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>vendor-specific</td>
<td>Set to v if this is a vendor-specific option, or omit otherwise.</td>
</tr>
<tr>
<td>option</td>
<td>Set to the DHCP option in the format, nnn.</td>
</tr>
<tr>
<td>offset</td>
<td>Set to a period followed by the number of bytes into the option where the</td>
</tr>
<tr>
<td></td>
<td>value is located, or a plus-sign (+) to indicate a list of values in the</td>
</tr>
<tr>
<td></td>
<td>DHCP option – each to be mapped to an instance of the RADIUS attribute.</td>
</tr>
</tbody>
</table>
The following are examples of DHCP option fields:

- `1ip` (The “Subnet Mask” option as an IP address)
- `3+ip` (The “Router” option as a list of IP address, each to be mapped to an instance of the RADIUS attribute)
- `6.4ip` (The “DNS Server” option as a second IP address in list (each IP address is 4 bytes))
- `12s` (The “Host Name” as a string)

The RADIUS attribute can be set to the name of any attribute defined in any dictionary. A literal value can be specified instead of a RADIUS attribute. This value must be text enclosed in double-quotes (“”).

The string is interpreted based on the format of the DHCP option:

- IP addresses must be specified in dotted notation; for example, 127.0.0.1 for IPv4 networks.
- Integers are expressed in decimal format; for example, 100.
- Strings are expressed as any text sequence.

The text can include escape sequences, where the backslash character (\) is the escape character. Table 68 lists escape sequences.

### Table 67: `pool.dhc` [Request] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>format</td>
<td>Set to the format of the DHCP option, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td><code>n32</code> a 32-bit integer</td>
</tr>
<tr>
<td></td>
<td><code>n16</code> a 16-bit integer</td>
</tr>
<tr>
<td></td>
<td><code>n8</code> an 8-bit integer</td>
</tr>
<tr>
<td></td>
<td><code>s</code> or <code>string</code> a string</td>
</tr>
<tr>
<td></td>
<td><code>i</code> or <code>ip</code> an IP address</td>
</tr>
</tbody>
</table>

### Table 68: Escape Code Sequences

<table>
<thead>
<tr>
<th>Escape Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\a</code></td>
<td>7</td>
</tr>
<tr>
<td><code>\b</code></td>
<td>8</td>
</tr>
<tr>
<td><code>\f</code></td>
<td>12</td>
</tr>
<tr>
<td><code>\n</code></td>
<td>10</td>
</tr>
<tr>
<td><code>\r</code></td>
<td>13</td>
</tr>
<tr>
<td><code>\t</code></td>
<td>9</td>
</tr>
<tr>
<td><code>\v</code></td>
<td>11</td>
</tr>
<tr>
<td><code>\mm</code></td>
<td>A decimal value between 0 and 255.</td>
</tr>
<tr>
<td><code>\xmm</code></td>
<td>A hexadecimal value between 00 and FF</td>
</tr>
</tbody>
</table>
An escape sequence can be used to set an option to an arbitrary binary value. This is useful, for example, when setting the Vendor Class Identifier option (60).

The following example sets the DHCP Host Name option to the RADIUS Calling-Station-Id, and sets the DHCP Vendor Class Identifier option to a binary string:

```plaintext
[Request]
12s = Calling-Station-Id
60s = "\x01\x02\x03\x04\x05"
```

### [Reply] Section

The [Reply] section allows RADIUS Access-Accept attributes to be constructed from options the DHCP server returns in an ACK message, in the following way:

```plaintext
[Reply]
RADIUS attribute = DHCP option
RADIUS attribute = DHCP option
```

See the [Request] section for information on how to specify the RADIUS attribute and the DHCP option values.

**NOTE:** In contrast to the [Request] section, the left and right sides of the equal sign are reversed to account for the direction in which the data is being set.

The following example returns the RADIUS Framed-IP-Netmask attribute from the DHCP Subnet Mask option and sets the RADIUS Framed-MTU attribute from the DHCP Interface MTU option:

```plaintext
[Reply]
Framed-IP-Netmask = 1ip
Framed-MTU = 26n16
```

### Reconfiguring Pools

DHCP pool information is loaded at startup from the dhcp.ini file and all associated pool.dhc files. DHCP pools can be added, deleted, and modified dynamically by doing the following:
1. Modify the dhcp.ini file and the pool.dhc files as required.

2. Restart the RADIUS process/service:

   - **Solaris/Linux**: Issue the HUP signal to the Steel-Belted Radius process.
     `kill -HUP ProcessID`

   - **Windows**: Run RADHUP.EXE from the command shell.

Steel-Belted Radius reads the modified files and configures its DHCP pools.
Chapter 6
Accounting Configuration Files

This chapter describes the usage and settings for the Steel-Belted Radius accounting initialization (.ini) files, which enable, disable, and configure accounting features of the server. Initialization files are loaded at startup time, and reside in the Steel-Belted Radius directory.

account.ini File		 page 142
account.ini File

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE*
**Not Used By:** —

The account.ini file contains information that controls how RADIUS accounting attributes are logged to a comma-delimited text file by Steel-Belted Radius. Specifically, the account.ini file controls file creation settings, such as file creation frequency, maximum size, and default directory, and file content, such as what information is recorded for each received accounting request.

**[Alias/name] Sections**

The [Alias/name] sections of account.ini are used to associate attributes of different names, but identical meaning. For example, one network access device vendor might call an attribute **Acct-Octet-Pkt** and another might call it **Acct-Oct-Packets**, yet the two attributes mean the same thing.

Each [Alias/name] section permits you to map one RADIUS accounting attribute that is already being logged by Steel-Belted Radius to any number of other attributes. You can provide as many [Alias/name] sections as you want, using the following syntax for each section:

```
[Alias/name]
VendorSpecificAttribute = VendorSpecificAttribute = 
```

Each VendorSpecificAttribute in the list is logged to the name column in the accounting log file. Because you are listing these attributes in an [Alias/name] section, verify they are not listed in the [Attributes] section, or they will be logged to their own columns as well as the name column.

All of the attribute names that you reference in an [Alias/name] section must be defined in a dictionary file that is already installed on the Steel-Belted Radius server. This includes name and each VendorSpecificAttribute entry.

In the following example, the standard RADIUS attribute **Acct-Octet-Packets** is mapped to the vendor-specific attributes **Acct-Octet-Pkt** and **Acct-Oct-Packets**. Values encountered for all three attributes are logged in the Acct-Octet-Packets column in the accounting log file:
[Attributes] Section

The [Attributes] section of the `account.ini` file lists all the attributes logged for each received accounting request in the accounting log file. When you install Steel-Belted Radius, the `account.ini` file is set up so that all standard RADIUS attributes and all supported vendors' accounting attributes are listed.

You can change the order of columns in the accounting log file by rearranging the sequence of attributes in the [Attributes] section. You can delete or comment out any attributes that are not relevant to your billing system or which do not apply to the equipment that you are using. This lets you design the content and column order of any spreadsheets that you plan to create based upon the accounting log file.

The syntax is as follows:

```
[Attributes]
AttributeName=
AttributeName=
...
```

For example:

```
[Attributes]
User-Name=
NAS-Port=
Framed-IP-Address=
Acct-Status-Type=
Acct-Delay-Time=
Acct-Session-Id=
```

The [Attributes] section lists one `AttributeName` on each line. You must ensure that an equal sign (=) immediately follows each `AttributeName`, with no spaces in between. Improperly formatted entries are considered invalid and are ignored.

Each `AttributeName` in the [Attributes] section must be defined in a standard RADIUS dictionary file or a vendor-specific dictionary file on the Steel-Belted Radius server.

---

**NOTE:** The first six attributes in each log file entry (Date, Time, RAS-Client, Record-Type, Full-Name, and Auth-Type) are always enabled, and cannot be re-ordered or deleted. Therefore, these attributes do not appear in the `account.ini` file [Attributes] section.
**[Configuration] Section**

*Used by:* GEE, SPE, SPE + MIM, SPE + EAP  
*Not used by:* EE

**[Settings] Section**

Steel-Belted Radius writes all accounting data to the current accounting log file (*act*) until that log file is closed. After closing the file, Steel-Belted Radius opens a new one and begins writing accounting data to it. You can configure how often this rollover of the accounting log file occurs.

The naming conventions for accounting log files permit more than one file to be generated during a day. Table 71 lists the file naming conventions used for different rollover periods. In the examples below, \( y \) = year digit, \( M \) = month digit, \( d \) = day digit, \( h \) = hour digit, and \( m \) = minute digit. When more than one file is generated during a day, the sequence number \( _nnnnn \) starts at _00000 each day.

**Table 70: account.ini [Configuration] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| LogDir    | Sets the destination directory on the local host where accounting log files are stored.  

Default value is the Steel-Belted Radius directory.  

**NOTE:** You cannot write accounting log files to a mapped or shared drive.  

**NOTE:** With directed realms, you can maintain separate accounting log locations for each realm.

**Table 71: Accounting File Rollover**

<table>
<thead>
<tr>
<th>File Generation Method</th>
<th>File Naming Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default (24 hours)</td>
<td>yyyyMMdd.act</td>
</tr>
<tr>
<td>Non-24-hour rollover</td>
<td>yyyyMMdd_hhmm.act</td>
</tr>
<tr>
<td>Rollover due to size</td>
<td>yyyyMMdd_nnnnn.act</td>
</tr>
<tr>
<td>Rollover due to size or startup when non-24-hour time in effect</td>
<td>yyyyMMdd_hhmm_nnnnn.act</td>
</tr>
</tbody>
</table>

The [Settings] section of the account.ini file (Table 72) controls how entries are written to the accounting log file, and ensures the compatibility of these entries with a variety of database systems.

**Table 72: account.ini [Settings] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| BufferSize| The size of the buffer used in the accounting logging process, in bytes.  

Default value is 131072 bytes.
Table 72: account.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carryover</td>
<td>If set to 1, each time a new accounting log file is created, a start record for each session that is currently active is written to the file.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, the list is not written.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>Enable</td>
<td>If set to 1, the accounting log feature is enabled.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, no .act files are created on this server.</td>
</tr>
<tr>
<td></td>
<td>Accounting servers should have Enable set to 1; for efficiency, non-accounting servers should have Enable set to 0.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>LineSize</td>
<td>Number in the range 1024–32768 that specifies the maximum size of a single accounting log line.</td>
</tr>
<tr>
<td></td>
<td>Default value is 4096.</td>
</tr>
<tr>
<td>LogFilePermissions</td>
<td>Specifies the owner and access permission setting for the accounting log file.</td>
</tr>
<tr>
<td></td>
<td>Enter a value for the LogFilePermissions setting in owner:group permissions format, where:</td>
</tr>
<tr>
<td></td>
<td>owner specifies the owner of the file in text or numeric format.</td>
</tr>
<tr>
<td></td>
<td>group specifies the group setting for the file in text or numeric format.</td>
</tr>
<tr>
<td></td>
<td>permissions specifies what privileges can be exercised by Owner/Group/Other with respect to the file in text or numeric format.</td>
</tr>
<tr>
<td></td>
<td>For example, ralphw:1007 rw------- specifies that the file owner (ralphw) can read and edit the log file, members of group 1007 can read (but not edit) the log file, and that other users cannot access the log file.</td>
</tr>
<tr>
<td>MaxSize</td>
<td>The maximum size of an accounting log file, in bytes.</td>
</tr>
<tr>
<td></td>
<td>If the accounting log file reaches or exceeds this size when it is checked, the log file is closed and a new file started. A value of 0 (the default) means unlimited size.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Because the size of the log file is checked once per minute, the log file can exceed the maximum size specified in this parameter.</td>
</tr>
<tr>
<td>QuoteBinary</td>
<td>If set to 1, binary values written to the accounting log file are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the accounting application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>QuoteInteger</td>
<td>If set to 1, integer values written to the accounting log file are enclosed in quotes.</td>
</tr>
<tr>
<td></td>
<td>If set to 0, quotes are not used.</td>
</tr>
<tr>
<td></td>
<td>Set this value according to the format expected by the accounting application that processes the entries.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
</tbody>
</table>
### Table 72: account.ini [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| QuoteIPAddress  | - If set to 1, IP addresses written to the accounting log file are enclosed in quotes.  
|                 | - If set to 0, quotes are not used.  
|                 | Set this value according to the format expected by the accounting application that processes the entries.  
|                 | Default value is 1. |
| QuoteText       | - If set to 1, text strings written to the accounting log file are enclosed in quotes.  
|                 | - If set to 0, quotes are not used.  
|                 | Set this value according to the format expected by the accounting application that processes the entries.  
|                 | Default value is 1. |
| QuoteTime       | - If set to 1, time and date values written to the accounting log file are enclosed in quotes.  
|                 | - If set to 0, quotes are not used.  
|                 | Set this value according to the format expected by the accounting application that processes the entries.  
|                 | Default value is 1. |
| RollOver        | Specifies how often the current accounting log file is closed and a new file opened (a rollover), up to one rollover per minute. Non-zero values indicate the number of minutes until the next rollover.  
|                 | If set to 0, the accounting log file rolls over once every 24 hours, at midnight local time.  
|                 | Default value is 0. |
| RollOverOnStartup| - If set to 1, each time Steel-Belted Radius is started, it closes the current accounting log file and opens a new one. A sequence number \_nnnnn is appended to the log file name, just as when MaxSize is reached.  
|                 | - If set to 0, each time Steel-Belted Radius is started, it appends entries to the previously open accounting log file.  
|                 | Default value is 0. |
| Titles          | - If set to 1, each time a new accounting log file is created, the title line (containing column headings) is written to the file.  
|                 | - If set to 0, the line is not written.  
|                 | Default value is 1. |
| UTC             | - If set to 1, time and date values are provided according to Universal Time Coordinates (UTC, formerly known as Greenwich Mean Time or GMT).  
|                 | - If set to 0, time and date values reflect local time.  
|                 | Default value is 0. |
**[TypeNames] Section**

Each entry in the [TypeNames] section of account.ini maps a possible value of the Acct-Status-Type attribute to a string. The value of this attribute is written into the fourth column of each accounting log record.

The syntax is as follows:

```
[TypeNames]
TypeID = TypeName
TypeID = TypeName
...
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TypeID</td>
<td>Each <code>TypeID</code> is a numeric value that corresponds to a possible value of the Acct-Status-Type attribute. This attribute appears in every incoming RADIUS accounting packet to identify the types of data it is likely to contain.</td>
</tr>
<tr>
<td>TypeName</td>
<td>Each <code>TypeName</code> value is a string. This string is written to the accounting log to identify the type of packet.</td>
</tr>
</tbody>
</table>

The standard Acct-Status-Type values 1, 2, 3, 7, and 8 are already listed in the [TypeNames] section of account.ini as follows:

```
[TypeNames]
1=Start
2=Stop
3=Interim
7=On
8=Off
```

You can edit the [TypeNames] section to add vendor-specific packet types to this list, which makes your accounting log files easier to read and use. For example:

```
[TypeNames]
1=Start
2=Stop
3=Interim
7=On
8=Off
639=AscendType
28=3ComType
```

If no string is given for a particular Acct-Status-Type, Steel-Belted Radius uses the numeric value of the incoming Acct-Status-Type attribute, formatted as a string.
This chapter describes the configuration files relating to proxy and directed realm administration in Steel-Belted Radius.

Table 74 lists the files in the Steel-Belted Radius directory you must edit to configure realms.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius.ini</td>
<td>Enables and disables realm features.</td>
</tr>
<tr>
<td>proxy.ini</td>
<td>Specifies the order of realm selection methods, the realm selection rules, and other settings for all realms on the server.</td>
</tr>
<tr>
<td>RealmName.pro</td>
<td>For each proxy realm that you want to configure on the Steel-Belted Radius server, you must create a file called <code>RealmName.pro</code>, where <code>RealmName</code> is the name of the realm, and you must register this RealmName by listing it in the [Realms] section of the <code>proxy.ini</code> file.</td>
</tr>
<tr>
<td>RealmName.dir</td>
<td>For each directed authentication and/or accounting realm that you want to configure on the Steel-Belted Radius server, you must create a file called <code>RealmName.dir</code>, where <code>RealmName</code> is the name of the realm, and you must register this RealmName by listing it in the [Directed] section of <code>proxy.ini</code>.</td>
</tr>
<tr>
<td>filter.ini</td>
<td>Stores filters for RADIUS attributes; these filters may be referenced from the [Auth] or [Acct] section of a <code>RealmName.pro</code> or <code>RealmName.dir</code> file. NOTE: Do not edit the <code>filter.ini</code> file manually. Use the SBR Administrator to configure rules for filtering RADIUS attributes.</td>
</tr>
</tbody>
</table>

NOTE: Do not edit the `filter.ini` file manually. Use the SBR Administrator to configure rules for filtering RADIUS attributes.
Proxy Realm Configuration Files

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM  
**Not used by:** EE

This section describes how to set up the proxy realm configuration files.

**Sample radius.ini Realm Settings**

The following settings in your radius.ini file enables the realm feature and the attribute filtering feature. These two features must be enabled for the sample proxy realm configuration files to work:

```ini
[Configuration]
ExtendedProxy=1
AttributeEdit=1
```

**NOTE:** For radius.ini syntax details, see “[Configuration] Section” on page 26.

**Examples**

The following proxy.ini file registers a proxy realm called sample.com and adds that realm to the list of target realms for static proxy accounting.

```ini
[Realms]
sample.com

[StaticAcct]
7=CustAOnOff  
8=CustAOnOff

[CustAOnOff]
realm=sample.com
```

**NOTE:** For syntax details, see “proxy.ini File” on page 155.

The following proxy.ini file entry specifies that otto@rtt.other.com and carol@3g.other.com would both map to the other.com proxy realm.

```ini
[Realms]
other.com = *.other.com
```

The following proxy.ini file specifies that otto@rtt.other.com and carol@3g.other.com would map to the other.com proxy realm and that caitlin@groton.other.com would map to the groton.other.com proxy realm.

```ini
[Realms]
other.com = *.other.com
groton.other.com
```
Sample Proxy RADIUS (.pro) File

The following complete file must be called sample.com.pro for it to work with the sample proxy.ini file shown on page 150.

```
[Auth]
Enable = 1
TargetsSection = AuthTargets
RoundRobin = 2
StripRealm = 0
RequestTimeout = 5
NumAttempts = 3
FilterOut = CustAOut
FilterIn = CustAIn
MessageAuthenticator = 0
UseMasterDictionary = yes

[Acct]
Enable = 1
TargetsSection = AcctTargets
RoundRobin = 1
StripRealm = 0
RequestTimeout = 5
NumAttempts = 3
FilterOut = CustAOut
: FilterIn =
: RecordLocally = 1
: Block = 1
UseMasterDictionary = yes

[AuthTargets]
bunion=1
desktop=1

[AcctTargets]
desktop

[Called-Station-ID]
8885551212
5551234

[FastFail]
MinFailures = 3
MinSeconds = 3
ResetSeconds = 30
```

NOTE: For syntax details, see “Proxy RADIUS Configuration (.pro) File” on page 164.

This example expects the Steel-Belted Radius database to contain Proxy entries with target names Desktop and Bunion. These entries are required to provide the network routing information (IP address, RADIUS shared secret, and UDP ports) that allows forwarded packets to reach the target servers at the customer site.
**Sample filter.ini File**

The following complete sample filter.ini file defines the two attribute filters referenced in the sample.com.pro file shown on page 151.

```
[CustAOut]
ALLOW
EXCLUDE NAS-IP-Address
ADD NAS-IP-Address 1.2.3.4
```

```
[CustAIn]
EXCLUDE
ALLOW Session-Timeout
ALLOW Idle-Timeout
ALLOW Service-Type Framed
ADD Service-Type Framed
ADD Framed-IP-Address CustAPool
```

The CustAOut filter in this example is designed to be applied to request packets coming into the Steel-Belted Radius server that are directed out to the realm. It allows all of the attributes in the packet to go out to the realm, with the exception of the RADIUS client’s IP address. It replaces this IP address with the specific “dummy” address 1.2.3.4. This filter enhances overall security by not publishing routing information to the network when it’s not necessary to do so.

The CustAIn filter in this example is designed to be applied to response packets returning to the Steel-Belted Radius server, which are relayed, in turn, to the RADIUS client. Most attributes are excluded; however, if any timeout values are returned, they’ll be allowed through. If the Service-Type attribute is present in the response and it has the value Framed (a string alias for the Service-Type integer value 2), it is allowed in the packet. Steel-Belted Radius adds the Service-Type attribute to the packet if it is not already there, and assigns it the value Framed (2).

The CustAIn filter in this example expects the Steel-Belted Radius database to contain an IP address pool entry called CustAPool, which specifies the customer’s valid address ranges. If this entry is not present, the CustAIn filter fails. CustAPool is referenced in the filter’s final entry, which assigns a value to the Framed-IP-Address attribute. As shown in the example, this entry causes Steel-Belted Radius to (1) add the Framed-IP-Address attribute to the packet; (2) select an available address from CustAPool, and (3) assign this value to the Framed-IP-Address attribute.
Directed Realm Configuration Files

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM  
**Not used by:** EE

This section discusses how to set up the directed realm configuration files.

**Sample radius.ini Realm Settings**

The same `radius.ini` excerpt works for our sample directed realm as for our sample proxy realm. The ExtendedProxy setting needs to be enabled (set to 1). The AttributeEdit setting does not apply to directed realms.

```ini
[Configuration]
ExtendedProxy=1
```

**NOTE:** For syntax details, see “[Configuration] Section” on page 26.

**Sample proxy.ini File**

The following `proxy.ini` file registers the proxy realm called `sample.com` and registers a directed authentication and/or accounting realm called `sample2.com`. It defines several directed accounting methods, including those we plan to reference from the `sample2.com.pro` realm configuration file.

```ini
[Realms]
sample.com

[Directed]
sample2.com

[DirectedAcctMethods]
CustBAcctSQL = c:\radius\CustomerB\theirsql.acc
CustCAcctAttributes = c:\radius\CustomerC\account.ini
CustCAcctSQLConfig = c:\radius\CustomerC\sqlacct.acc
CustDAcctSQLConfig3 = c:\radius\CustomerD\mysql.acc
```

**NOTE:** For syntax details, see “proxy.ini File” on page 155.

The following `proxy.ini` file specifies that `otto@rtt.other.com` and `carol@3g.other.com` would both map to the `other.com` directed realm.

```ini
[Directed]
other.com = *.other.com
```
The following proxy.ini file specifies that \texttt{otto@rtt.other.com} and \texttt{carol@3g.other.com} would map to the \texttt{other.com} directed realm and that \texttt{caitlin@groton.other.com} would map to the \texttt{groton.other.com} directed realm.

```
[Directed]
other.com = *.other.com
groton.other.com
```

**Sample Directed Realm (.dir) File**

The following configuration file must be called \texttt{sample2.com.dir} for it to work with the sample \texttt{radius.ini} file (described on page 153) and \texttt{proxy.ini} file (described on page 153).

```
[Auth]
Enable = 1
StripRealm = 1
UseMasterDictionary = yes

[Acct]
Enable = 1
RecordLocally = 1
UseMasterDictionary = yes

[AuthMethods]
Native User

[AcctMethods]
CustCAcctAttributes
CustCAcctSQLConfig

[Called-Station-Id]
8885551212
55512340
```

\textbf{NOTE:} For syntax details, see “Directed Realm Configuration (.dir) File” on page 176.

This sample file configures both directed authentication and directed accounting. It also strips realm routing information from the User-Name prior to authentication.

The [Acct Methods] section of this file lists the two accounting methods for the \texttt{sample2.com} realm. These are \texttt{CustCAcctAttributes}, which specifies how to log attributes to a .act accounting log file on the local server, and \texttt{CustCAcctSQLConfig}, which configures accounting to an external SQL database. Both methods are configured in the [DirectedAcctMethods] section of our sample \texttt{proxy.ini} file, above.
proxy.ini File

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM*
**Not used by:** EE

The `proxy.ini` file specifies the order of realm selection methods, the realm selection rules, and other settings for all realms on the server. Settings for a realm are provided in its `RealmName.pro` or `RealmName.dir` file.

After you edit `proxy.ini`, you must apply your changes as follows:

- If you’ve configured any proxy realms, you can load your new realm configuration without stopping and restarting the server.
  - **Solaris/Linux**: Issue the `HUP` signal to the Steel-Belted Radius process. `kill -HUP ProcessID`
  - **Windows**: Run `RADHUP.EXE` from the command shell.

Steel-Belted Radius re-reads `proxy.ini`, `filter.ini`, and all `*.pro` and `*.dir` files in the server directory, and resets its realm configuration.

- If you’ve configured any directed realms and if you’ve added or changed:
  - **Any directed accounting methods**: you must stop and restart the server to load your new configuration.
  - **Directed authentication methods in which external database (SQL or LDAP) authentication is used**, you must stop and restart the server to load your new configuration.
  - **Directed authentication methods in which local or pass-through (Native, UNIX, Domain, Host, SecurID, or TACACS+) authentication is used**, you can load your realm configuration by using a HUP signal.

**[Configuration] Section**

The `[Configuration]` section of `proxy.ini` permits you to define prefix and suffix conventions for realm name parsing and specifies whether to use the master RADIUS dictionary to process inbound proxy responses.

You can enable prefix and suffix conventions for realm name parsing if you specify a different delimiter character for each. All prefixed name decorations must use the prefix delimiter, and all suffixed name decorations must use the suffix delimiter.

If you set the prefix and suffix delimiter to the same character, both prefix and suffix conventions are enabled, but (since suffixes are checked first) prefixes may be misinterpreted.

You should choose different delimiter characters for tunnels, proxies, and realms.
Table 75: proxy.ini [Configuration] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealmPrefix</td>
<td>Specifies the character used to identify prefixed name decorations; for example, RAS1/RAS2/joeuser.</td>
</tr>
<tr>
<td></td>
<td>Default value is /.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Enter \ to specify the backslash character, since a single backslash in a configuration file indicates a line continuation.</td>
</tr>
<tr>
<td>RealmSuffix</td>
<td>Specifies the character used to identify suffixed name decorations; for example, joeuser@RAS1@RAS2.</td>
</tr>
<tr>
<td></td>
<td>Default value is @.</td>
</tr>
<tr>
<td></td>
<td>NOTE: Enter \ to specify the backslash character, since a single backslash in a configuration file indicates a line continuation.</td>
</tr>
<tr>
<td>UseMasterDictionary</td>
<td>■ If set to yes, inbound proxy responses use the master Steel-Belted Radius dictionary when attributes are filtered in.</td>
</tr>
<tr>
<td></td>
<td>■ If set to no, proxy responses use the client-specific dictionary when attributes are filtered in.</td>
</tr>
<tr>
<td></td>
<td>Default value is yes.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The UseMasterDictionary setting configured in individual .dir or .pro files overrides the global setting configured in the proxy.ini file.</td>
</tr>
</tbody>
</table>

[Realms] Section

The [Realms] section of proxy.ini lists all of the proxy realms known to the server. The syntax is as follows:

```
[Realms]
RealmName
RealmName [= match_rule]
RealmName [= <undecorated>]
```

Table 76: proxy.ini [Realms] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealmName</td>
<td>Each entry must match the name of a RealmName.pro file in the same directory as proxy.ini.</td>
</tr>
<tr>
<td>[= match_rule]</td>
<td>Optional. Specifies a rule for mapping the domain information in a User-Name to a proxy realm by means of prefix or suffix wildcards</td>
</tr>
<tr>
<td>[= &lt;undecorated&gt;]</td>
<td>Optional. Marker indicating the specified realm is used to process requests containing undecorated User-Name information.</td>
</tr>
</tbody>
</table>

[Directed] Section

The [Directed] section of proxy.ini (Table 77) lists the names of all of the directed authentication and/or accounting realms on the server. The syntax for the [Directed] section is as follows:

```
[Directed]
RealmName
RealmName [= match_rule]
RealmName [= <undecorated>]
```

Chapter 7: Realm Configuration Files

Table 77: proxy.ini [Directed] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealmName</td>
<td>Each entry must match the name of a RealmName.dir file in the same directory as proxy.ini.</td>
</tr>
<tr>
<td>= match_rule</td>
<td>Optional. Specifies a rule for mapping the domain information in a User-Name to a directed realm by means of prefix or suffix wildcards.</td>
</tr>
<tr>
<td>= &lt;undecorated&gt;</td>
<td>Optional. Marker indicating the specified realm is used to process requests containing undecorated User-Name information.</td>
</tr>
</tbody>
</table>

[Processing] Section

If this section is present, it lets you specify which realm selection rules are applied and the order in which they are applied. If no [Processing] section is present, routing continues in its default behavior.

NOTE: If the script keyword appears in the [Processing] section, Steel-Belted Radius executes the realm selection script first, before trying other built-in methods. For more information, refer to the Steel-Belted Radius Scripting Guide.

<table>
<thead>
<tr>
<th>[Processing]</th>
<th>RealmSelector</th>
</tr>
</thead>
</table>

Table 78: proxy.ini [Processing] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealmSelector</td>
<td>This can be one of five identifiers: Attribute-Mapping, DNIS, Prefix, Suffix, or Undecorated. Only the rules corresponding to the values listed are applied, and they are applied in the order you specify them.</td>
</tr>
</tbody>
</table>

The following example enables undecorated User-Names, suffix delimiters, prefix delimiters, and DNIS rules (in that order).

[Processing]
Suffix
Prefix
DNIS
Undecorated

[AttributeMap] Sections

The [AuthAttributeMap] and [AcctAttributeMap] sections of proxy.ini let you map the presence, absence, or specific value of an attribute in the incoming packet to a specific realm. This is referred to as attribute mapping.
An [AuthAttributeMap] or [AcctAttributeMap] section consists of one or more \textit{RealmName} entries. Each \textit{RealmName} must match the name of a realm configuration file (\textit{RealmName}.pro or \textit{RealmName}.dir) in the same directory as \texttt{proxy.ini}.

\textbf{NOTE:} Attribute mapping is supported by proxy realms and directed realms. You cannot use this feature when forwarding packets to a proxy target that is not accessed through a realm.

Each \textit{RealmName} entry is a list of statements that can be true or false regarding the attributes in an incoming RADIUS packet; we call these statements \textit{rules}. Rules found in [AuthAttributeMap] apply to authentication packets; rules found in [AcctAttributeMap] apply to accounting packets. In all other respects, [AuthAttributeMap] or [AcctAttributeMap] are the same. The syntax for individual rules may vary; the following example shows all of the possible syntax variations:

\begin{verbatim}
[AuthAttributeMap]
RealmName
  Attribute=Value
  Attribute~Attribute=Value
  ~Attribute
  ...

[AcctAttributeMap]
  ...
\end{verbatim}

For example:

\begin{verbatim}
[AuthAttributeMap]
  CustTRealm
    Framed-Protocol=1
    Service-Type=2
  CustQRealm
    Framed-Protocol=PPP
    ~Service-Type=Framed
  NativeRealm
\end{verbatim}

Each attribute mapping rule must begin with a space or tab character, followed optionally by a tilde (~), then the name of a standard or vendor-specific RADIUS Attribute that is in one of the Steel-Belted Radius dictionary files. If a Value is present, it is preceded by an equal sign (=), and must specify a valid possible value for that attribute. The rule is terminated by a carriage return. Tilde (~) indicates that the rule is satisfied only if the attribute or attribute/value pair is not present in the packet.

Each \textit{RealmName} entry in an [AuthAttributeMap] or [AcctAttributeMap] section is examined in sequence from top to bottom. Within each \textit{RealmName} entry, each rule is evaluated in sequence from top to bottom. The results are as follows:

- If all of the rules in a \textit{RealmName} entry evaluate to \textit{true}, the packet is routed to the realm called \textit{RealmName} and the remaining entries in the attribute map are ignored.
- If any of the rules in a **RealmName** entry evaluate to **false**, this entry does not result in a mapping. Steel-Belted Radius evaluates the next entry in the map.

- If Steel-Belted Radius encounters a **RealmName** entry that contains no rules, the packet is automatically directed to that realm.

Table 79 explains how the various types of rules are evaluated.

<table>
<thead>
<tr>
<th>Syntax Variation</th>
<th>Function of the Attribute Mapping Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute=Value</td>
<td>If the <strong>Attribute</strong> is present in the request packet and it has the <strong>Value</strong> shown, then this rule is true. If the <strong>Attribute</strong> is not present, or if it is present but does not have the <strong>Value</strong> shown, then this rule is false.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The Steel-Belted Radius dictionary file radius.dct provides string aliases for certain integer values defined in the RADIUS standard. You can use these strings in attribute mapping rules.</td>
</tr>
<tr>
<td>Attribute</td>
<td>If the <strong>Attribute</strong> is present in the request packet, then regardless of its value, this rule is true. If the <strong>Attribute</strong> is not present, then this rule is false.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>You won’t often use the Attribute rule without a Value, because most of the RADIUS packets coming into your configuration are going to contain the same set of RADIUS attributes, but with different Values.</td>
</tr>
<tr>
<td>~Attribute=Value</td>
<td>Note the tilde (~) operator. This rule is looking for a specific attribute that may have any value except the one listed. If <strong>Attribute</strong> is present in the request packet and it does not have the <strong>Value</strong> shown, then this rule is true. If <strong>Attribute</strong> is not present, or if it is present but does have the <strong>Value</strong> shown, then this rule is false.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The following is not valid syntax: <strong>Attribute=~Value</strong></td>
</tr>
<tr>
<td>~Attribute</td>
<td>Note the tilde (~) operator and the absence of a Value. If <strong>Attribute</strong> is not present in the request packet, then this rule is true. If <strong>Attribute</strong> is present, then this rule is false.</td>
</tr>
</tbody>
</table>

When setting up [AuthAttributeMap] or [AcctAttributeMap] rules for your configuration, you should distinguish between the different realms whose requests you are processing. Consider how specific your rules must be to identify each realm uniquely. Is the presence of a particular attribute sufficient (**Ascend-IP-Address**), or must the attribute have a specific value before you can be sure of its source (**NAS-IP-Addr=n.n.n.n**)? Make sure that your logic does not permit a crossing of requests between realms.

If a realm destination has been identified by applying an [AuthAttributeMap] entry to the attributes in a session’s authentication request, Steel-Belted Radius uses the same realm for that session’s accounting requests (if the realm is enabled for accounting). Generally, this is the desired behavior for the realm. You should provide an [AcctAttributeMap] entry only if there is no [AuthAttributeMap] entry for a realm and you want to map the realm using one or more accounting attributes.
[DirectedAcctMethods] Section

The [DirectedAcctMethods] section of the proxy.ini file lists one or more external database accounting configuration files (.acc) or local accounting initialization files (.ini) on the local server, and assigns each of these files a name by which it may be referenced in a RealmName.dir file.

The syntax for the [DirectedAcctMethods] section is as follows:

```ini
[DirectedAcctMethods]
Description=PathAndFile
Description=PathAndFile
:
```

where Description is the name by which you want to reference the accounting method and PathAndFile is the full pathname of a .acc or .ini file on the local server.

- Solaris/Linux:
  ```
  /usr/lib/extras/acctlib.acc
  /usr/lib/extras/ouracct.ini
  ```

- Windows:
  ```
  c:\radius\extras\acctlib.acc
  c:\radius\extras\ouracct.ini
  ```

This is the file that implements the accounting method. The location of this file must not be the Steel-Belted Radius directory.

- If your PathAndFile identifies a .acc file, external database accounting is performed as configured in the file. You may reference the Steel-Belted Radius SQL accounting module in the [Bootstrap] section of this .acc file.

- If your PathAndFile identifies a .ini file, you may omit the [Bootstrap] section from this file. Normal Steel-Belted Radius logging is performed, except that:
  - Accounting log entries (for requests that are routed to this accounting method) are written to accounting log files (.act) in the specified Path, rather than in the server directory.
  - Logging details (which attributes are logged, and in which order) are controlled by the [Settings] and [Attributes] sections of the .ini file listed in PathAndFile, rather than the account.ini file found in the server directory.

[StaticAcct] Section

Static proxy accounting lets you send duplicate copies of certain types of accounting request to proxy realms (or any RADIUS-aware device), in addition to the normal routing of the original accounting request. The number of duplicates is not limited.

The [StaticAcct] section of proxy.ini maps possible values of the Acct-Status-Type attribute to a list of proxy realms that receive statically-forwarded, duplicate copies of all accounting packets of that type.
Acct-Status-Type is a RADIUS standard attribute that identifies the type of accounting request. Table 80 lists the names and meanings assigned to Acct-Status-Type values 1, 2, 3, 7, and 8. Additional values for Acct-Status-Type have been defined by network access device vendors for use with their equipment; you can also use these values in the [StaticAcct] section.

Table 80: Acct-Status-Type Attribute Values

<table>
<thead>
<tr>
<th>Acct-Status-Type Value</th>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start</td>
<td>A user session has started</td>
</tr>
<tr>
<td>2</td>
<td>Stop</td>
<td>A user session has stopped, request contains final statistics</td>
</tr>
<tr>
<td>3</td>
<td>Interim</td>
<td>A user session is in progress, request contains current statistics</td>
</tr>
<tr>
<td>7</td>
<td>Accounting-On</td>
<td>The network access device has started</td>
</tr>
<tr>
<td>8</td>
<td>Accounting-Off</td>
<td>The network access device is about to shut down</td>
</tr>
</tbody>
</table>

The syntax for a [StaticAcct] section is as follows:

```
[StaticAcct]
number=name
number=name
::
```

where each `number` is a possible value of the Acct-Status-Type attribute, and each `name` identifies a section called `[name]` that appears elsewhere in the `proxy.ini` file.

When it receives an accounting request with an Acct-Status-Type of `number`, Steel-Belted Radius uses the [StaticAcct] section to match `number` with `name`, and statically forwards a duplicate copy of the packet to all of the proxy realms listed in the `[name]` section.

Each `[name]` section consists of a list name in square brackets ([`name`]) followed by a list of proxy realms. Each of these realms must have a `RealmName.pro` file in the same directory as `proxy.ini`. Directed realms do not support static proxy accounting.

The syntax for a `[name]` section is as follows:

```
[name]
realm=RealmName
realm=RealmName
::
```

The `[name]` section is used only if its `name` is mapped to a number in the [StaticAcct] section of the `proxy.ini` file.

The following excerpt from a `proxy.ini` file demonstrates some of the flexibility of static proxy forwarding. Copies of all session-related accounting packets (Start, Stop, and Interim) are proxy-forwarded to a realm called billing. Copies of all device-related accounting packets (Accounting-On and Accounting-Off) are proxy-forwarded, not only to billing, but also to a realm called operations.
[Realms]
billing
operations

[StaticAcct]
1 = SessionObserverList
2 = SessionObserverList
3 = SessionObserverList
7 = RASObserverList
8 = RASObserverList

[SessionObserverList]
realm = billing

[RASObserverList]
realm = billing
realm = operations

[Interfaces] Section

If your server has more than one network interface, you can assign the outgoing proxy traffic for a particular realm to a particular interface card:

1. List the IP addresses associated with each network interface card in the [Addresses] section of the radius.ini file.

2. Create an [Interfaces] section for the proxy.ini file. This should consist of a list of one or more pairs in the following format:

   [Interfaces]
   InterfaceName = IPAddress
   where InterfaceName is a label you assign to the given IPAddress.

3. Extend the existing entries in the [name] sections in .pro files for proxy realms with the InterfaceName defined in the [Interfaces] section so that they are in the following format:

   [TargetSection]
   Target=NumAttempts,InterfaceName
   where InterfaceName is the name of the interface defined above in the [Interfaces] section.

For example:

   [Targets]
   Bert=3,ABCInterface
   Ernie=1,XYZInterface

**NOTE:** The ProxySource setting in the [Configuration] section of radius.ini disables per-realm control of proxy outbound interfaces. If ProxySource is not set, sockets are opened and bound for each interface on the server.
Proxyrl.ini File

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM  
**Not used by:** EE

The *proxyrl.ini* file supports a feature called *smart static accounting*, which lets you specify that the accounting packets for a proxy or directed realm should be forwarded to a list of one or more proxy realms. These groups of realms can also be used for static accounting configured in *proxy.ini*.

This file consists of a number of sections that you name. Each section name is referenced in the *StaticAcctRealms* parameter in the [Acct] section of a .pro or .dir file. Following the section name, you can list a number of proxy realm names, in the following format:

```
[realm-list-name-1]
proxy-realm-1
proxy-realm-2
...

[realm-list-name-2]
...
```

For example:

```
[StaticAcctTargets1]
AcctSrvr1
AcctSrvr4
```

NOTE: You must be sure that the list of static accounting servers doesn’t include any realms that use the list or an infinite loop occurs. If a realm that is included in a realm’s list of static accounting servers and is specified in *proxy.ini* as doing static accounting, it gets duplicate accounting packets.
Proxy RADIUS Configuration (.pro) File

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM  
**Not used by:** EE

For each proxy realm that you want to configure on the Steel-Belted Radius server, you must create a file called `RealmName.pro`, where `RealmName` is the name of the realm, and you must add this RealmName to the [Realms] section of the `proxy.ini` file.

If you create or edit a `RealmName.pro` file, you can apply your configuration changes dynamically, without stopping the server.

- **Solaris/Linux:** Issue the HUP signal to the Steel-Belted Radius process.  
  `kill -HUP ProcessID`

- **Windows:** Run `RADHUP.EXE` from the command shell.

After you do this, Steel-Belted Radius re-reads `proxy.ini`, `filter.ini`, and all `.pro` and `.dir` files in the server directory, and resets its realm configuration accordingly.

If you edit `radius.ini` while configuring a realm, you must stop and restart Steel-Belted Radius to load your new configuration.

### [Auth] Section

The [Auth] section of a `RealmName.pro` file (Table 81) configures authentication for the proxy realm. The key parameters in these sections are:

- **TargetsSection**, which names the target selection strategy you want to use.
- **FilterIn** and **FilterOut**, which name the attribute filters you want applied to request and response packets, respectively.

#### Table 81: RealmName.pro [Auth] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable          | ■ If set to 1, enables forwarding of authentication packets to the realm called `RealmName`.  
                 | ■ If set to 0, the realm called `RealmName` is disabled for authentication.  
                 | Default value is 0.                                                      |
| `FilterOut = name` | The `FilterOut = name` parameter causes Steel-Belted Radius to apply the filtering rules found in the [name] section of `filter.ini`.  
                          These rules are applied while Steel-Belted Radius is processing the incoming RADIUS request packet, and before it directs the packet “out” to the destination realm. You may also think of this as filtering various attributes and values “out” of the request before directing it to the realm. |
### Table 81: RealmName.pro [Auth] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>FilterIn = name</td>
<td>The <code>FilterIn=\textit{name}</code> parameter causes Steel-Belted Radius to apply the filtering rules found in the [\textit{name}] section of filter.ini. These rules are applied after Steel-Belted Radius has received a response “in” from the destination realm, and while it is preparing the RADIUS response packet for its client. You may also think of this as filtering various attributes and values “in” to the response before returning it to the client.</td>
</tr>
<tr>
<td>MessageAuthenticator</td>
<td>If set to 1, a Message-Authenticator is inserted into each request forwarded to any target server in the realm. Default value is 0. <strong>NOTE:</strong> Both the proxy and the target RADIUS server requires this functionality.</td>
</tr>
<tr>
<td>NumAttempts</td>
<td>The number of times a timeout may occur when attempting to contact servers within the realm, before a failure is declared and the attempts to forward the request are stopped. Default value is 3.</td>
</tr>
<tr>
<td>RequestTimeout = x, y, z</td>
<td>A list of times, in seconds, to wait when attempting to contact a target server before timing out. The first value is the time to wait before the first timeout, and so on. The number of items in the list should be no greater than the NumAttempts setting. If NumAttempts is greater, than the last number listed is reused for subsequent timeouts. Default value is 5. <strong>NOTE:</strong> You can specify RequestTimeout or RequestTimeoutMills, but not both.</td>
</tr>
<tr>
<td>RequestTimeoutMills = x, y, z</td>
<td>A list of times, in milliseconds, to wait when attempting to contact a target server before timing out. The first value is the time to wait before the first timeout, and so on. The number of items in the list should be no greater than the NumAttempts setting. If NumAttempts is greater, than the last number listed is reused for subsequent timeouts. <strong>NOTE:</strong> You can specify RequestTimeout or RequestTimeoutMills, but not both.</td>
</tr>
<tr>
<td>RoundRobin</td>
<td>Specifies the number of target servers that are participating in round-robin load balancing. The count begins from the top of the list in the [\textit{name}] section identified by TargetsSection. Other listed targets are used only after the round-robin targets fail for a particular request. Default value is 2.</td>
</tr>
</tbody>
</table>
| StripRealm              | - If set to 1, strip the realm name from the username before forwarding.  
- If set to 0, name stripping is disabled. **NOTE:** For proxy realms, realm name stripping is disabled (\textit{StripRealm = 0}) by default. If you want to enable it, you must explicitly set \textit{StripRealm} to 1. |
**Table 81: RealmName.pro [Auth] Syntax (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TargetsSection = name</td>
<td><em>name</em> identifies a section called [name] that appears elsewhere in the .pro file. This section lists all the targets in a proxy realm. When it receives a request for this proxy realm, Steel-Belted Radius selects a target from this list. Having the TargetsSection setting available in the [Auth] and [Acct] sections permits you to name different target selection parameters for proxy RADIUS authentication and accounting. Default value of <em>name</em> is AuthTargets, indicating the name of the section is [AuthTargets].</td>
</tr>
</tbody>
</table>
| UseMasterDictionary      | - If set to yes, inbound proxy responses for this realm use the master Steel-Belted Radius dictionary when authentication attributes are filtered in.  
- If set to no, proxy responses for this realm use the client-specific dictionary when authentication attributes are filtered in.  
Default value is yes  
**NOTE:** This value overrides the global setting configured in the UseMasterDictionary parameter in the proxy.ini file. |

[**Acct**] Section

The [Acct] section of a RealmName.pro file (Table 82) configures accounting. The key parameters in these sections are:

- **TargetsSection**, which names the target selection strategy you want to use.
- **FilterIn** and **FilterOut**, which name the attribute filters you want applied to request and response packets, respectively.

**Table 82: RealmName.pro [Acct] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | - If set to 1, enables forwarding of accounting packets to the realm called *RealmName*.  
- If set to 0, the realm called *RealmName* is disabled for accounting.  
Default value is 0. |
| Block     | - If set to 0, the Steel-Belted Radius server sends an accounting acknowledgement immediately (for example, after Steel-Belted Radius records an accounting message).  
- If set to 1, the Steel-Belted Radius server waits for a response from the target realm before sending an accounting acknowledgement.  
Default value is 1.  
**NOTE:** Set the Block parameter to 0 if your network access device is not able to deal with long acknowledgment delays to accounting requests gracefully. |
Table 82: RealmName.pro [Acct] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>FilterOut = name</td>
<td>The FilterOut= name parameter causes Steel-Belted Radius to apply the filtering rules found in the [name] section of filter.ini. These rules are applied while Steel-Belted Radius is processing the incoming RADIUS request packet, and before it directs the packet “out” to the destination realm. You may also think of this as filtering various attributes and values “out” of the request before directing it to the realm.</td>
</tr>
<tr>
<td>FilterIn = name</td>
<td>The FilterIn= name parameter causes Steel-Belted Radius to apply the filtering rules found in the [name] section of filter.ini. These rules are applied after Steel-Belted Radius has received a response “in” from the destination realm, and while it is preparing the RADIUS response packet for its client. You may also think of this as filtering various attributes and values “in” to the response before returning it to the client.</td>
</tr>
<tr>
<td>NumAttempts</td>
<td>Specifies the number of times a timeout may occur when attempting to contact servers within the realm, before a failure is declared and the attempts are stopped. Default value is 3.</td>
</tr>
<tr>
<td>RecordLocally</td>
<td>If set to 1, log the packet locally before forwarding. If set to 0, forward the packet and do not log locally. Default value is 1.</td>
</tr>
<tr>
<td>RequestTimeout = x, y, z</td>
<td>A list of times, in seconds, to wait when attempting to contact a target server before timing out. The first value is the time to wait before the first timeout, and so on. The number of items in the list should be no greater than the NumAttempts setting. If NumAttempts is greater, than the last number listed is reused for subsequent timeouts. <strong>NOTE:</strong> You can specify RequestTimeout or RequestTimeoutMills, but not both.</td>
</tr>
<tr>
<td>RequestTimeoutMills = x, y, z</td>
<td>A list of times, in milliseconds, to wait when attempting to contact a target server before timing out. The first value is the time to wait before the first timeout, and so on. The number of items in the list should be no greater than the NumAttempts setting. If NumAttempts is greater, than the last number listed is reused for subsequent timeouts. <strong>NOTE:</strong> You can specify RequestTimeout or RequestTimeoutMills, but not both.</td>
</tr>
<tr>
<td>RoundRobin</td>
<td>Specifies the number of target servers that are participating in “round-robin” load balancing. The count begins from the top of the list in the [name] section identified by TargetsSection. Other listed targets are only used after the round-robin targets fail for a particular request. Default value is 1.</td>
</tr>
<tr>
<td>StaticAcctRealms</td>
<td>If a setting is supplied for this parameter, accounting packets are forwarded to a list of realms. The setting given must be a section name defined in the proxyrl.ini file that lists the realms to which the accounting packets should be forwarded. See “Proxyrl.ini File” on page 163.</td>
</tr>
</tbody>
</table>
[AutoStop] Section

The [AutoStop] section of a realm configuration file permits you to activate the Proxy AutoStop feature. When this feature is enabled, an AutoStop request is automatically recorded and associated with the session in the current sessions database when the initial Accounting-Start message is received. This AutoStop message may be used later to simulate an Accounting-Stop message which is fed back into the request processing engine, causing it to be forwarded to the appropriate realms and for the normal processes of ending the user session to be enacted.

NOTE: As the AutoStop record is generated when the session begins, it is simply a duplicate of the original Start request and does not have access to information about the lifetime of the user’s actual activity.

NOTE: AutoStop records are not saved on persistent storage: this means that if Steel-Belted Radius is restarted, this information is lost and hence Accounting-Stop messages cannot be simulated for these user sessions.
Table 83: RealmName.pro [AutoStop] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable    | Set to 0 to disable AutoStop for the current realm.  
|           | Set to 1 to enable AutoStop for the current realm.  
|           | Default value is 0. |

Table 84 lists the parameters in other configuration files you must enable (set to 1) for AutoStop to operate.

Table 84: AutoStop Configuration Requirements

<table>
<thead>
<tr>
<th>File</th>
<th>Section</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>RealmName.pro</td>
<td>[Acct]</td>
<td>Enable</td>
</tr>
<tr>
<td>RealmName.pro</td>
<td>[Acct]</td>
<td>RecordLocally</td>
</tr>
<tr>
<td>radius.ini</td>
<td>[Configuration]</td>
<td>AcctAutoStopEnable</td>
</tr>
</tbody>
</table>

**[Called-Station-ID] Section**

The [Called-Station-ID] section of a RealmName.pro file allows the target realm to be selected based on DNIS. The [Called-Station-ID] section lists each DNIS string that identifies the realm. If this string is found in the Called-Station-Id attribute of an incoming RADIUS request, the request is assumed to be addressed to this realm.

The syntax is as follows:

```
[Called-Station-ID]
String
String
...
```

where String is a DNIS string.

For example:

```
[Called-Station-ID]
8005551212
8005551213
6175551212
```

You can also use wildcards, as in the following example:

```
[Called-Station-ID]
800*
508*
```
**Target Selection Rules**

Each [name] section of a RealmName.pro file specifies a set of rules that Steel-Belted Radius can use to select a target for proxy-forwarding within the proxy realm. Each [name] section consists of a list of target servers. For any particular request, if the first listed server fails to respond (or is presumed down), the other servers are tried in the order listed. A [name] section is activated by referencing it from the [Auth] and/or [Acct] sections.

### Table 85: Proxy Realm Target Selection

<table>
<thead>
<tr>
<th>To activate…</th>
<th>Use…</th>
</tr>
</thead>
<tbody>
<tr>
<td>a [name] section for authentication</td>
<td>TargetName = name in the [Auth] section</td>
</tr>
<tr>
<td>the same [name] section for accounting</td>
<td>TargetName = name in the [Acct] section</td>
</tr>
<tr>
<td>some [other] section for accounting</td>
<td>TargetName = other in the [Acct] section</td>
</tr>
</tbody>
</table>

The full syntax is as follows:

```plaintext
[Auth]
TargetsSection=nameB

[Acct]
TargetsSection=nameA

[nameA]
Server = n
Server = n
::

[nameB]
Server = n
Server = n
::
```

where Server is the name of a server that you’ve configured as a target for standard proxy RADIUS forwarding, and \( n \) is explained in the next section.

Server must match a Proxy entry in the Steel-Belted Radius database. This Proxy entry provides the address and shared secret for the target server. All other settings in the Proxy entry (retry policy, proxy accounting) are overridden by the settings that you configure in the RealmName.pro file.

---

**NOTE:** If your server has multiple interface cards, you may add a parameter referring to the interface to each line to order the outgoing proxy traffic for the realm through a particular interface. See “[Interfaces] Section” on page 162.
**Round-Robin Load Balancing**

If you have multiple target servers in a realm, you can select whether to use them in round-robin fashion (load balancing), primary/backup fashion, or a combination of both. The value of the `RoundRobin` entry in the [Auth] or [Acct] section indicates the number of targets that are to be used in round-robin fashion. The count begins from the top of list in the [name] section. Other listed targets are used only if the round-robin targets fail for a particular request. If `RoundRobin` is 0 or 1, all requests are routed to the first target in the [name] list, assuming that it is up, the others are tried in the order listed.

If `RoundRobin` is 2 or greater (say, \( n \)), each request is routed to a different target server, in rotation among the first \( n \) listed targets. Requests are then load-balanced evenly among those targets. For any particular request, if one target fails to respond, other targets are attempted. The round-robin targets are tried first; if they all fail to respond, any additional targets are then tried in the order in which they appear in the list.

In the following example, `RoundRobin` is 3. Under normal circumstances, requests are balanced in round-robin fashion among the first three targets. The first request goes to Bert; the next goes to Ernie; the next to George; the next to Bert; the next to Ernie; the next to George; and so on. If any of these servers go down at some point, the other two are tried, in list order. The fourth target (Mary) receives requests only when other targets are down.

```plaintext
[Auth]
RoundRobin=3
NumAttempts=8
TargetsSection=Targets

[Targets]
Bert=1
Ernie=1
George=1
Mary=5
```

**Selecting a Backup Server**

If `RoundRobin` is set to 0, Steel-Belted Radius makes a selection from the “other” servers in the list only if the primary server is down.

For example:

```plaintext
[Auth]
RoundRobin=0
NumAttempts=8
TargetsSection=Targets

[Targets]
Bert=1
Ernie=1
```

In this case, Bert is used until there is a problem; then Ernie becomes the server of second choice.
Realm Retry Policy

Each target selection rule in the [name] section permits you to name a target and assign it a numeric value:

```
[name]
Server = n
Server = n
```

The \[n\] setting indicates the number of times to retry requests to this target server when it doesn’t respond (when no response is received from the server within the amount of time set by RequestTimeout in the [Auth] or [Acct] section).

The number of attempts to all servers within the entire realm is given by the NumAttempts value in the [Auth] or [Acct] section. For example, let’s say that NumAttempts is 8 and there are three target servers, each with \[n\] set to 3:

```
[Auth]
NumAttempts=8
TargetsSection=Targets

[Targets]
Bert=3
Ernie=3
George=3
```

Let’s say that all three servers are down when a request comes into the realm. The first target (Bert) is tried 3 times; then the second target (Ernie) is tried 3 times; and the third target (George) is tried 2 times. At this point, the number of tries to all servers in the realm is 8, which equals NumAttempts. Steel-Belted Radius returns a failure response from the realm.

---

**NOTE:** A third attempt to George could not be made unless you edited the RealmName.pro file, increased NumAttempts to 9, and reloaded Steel-Belted Radius.

---

**[FastFail] Section**

The [FastFail] section of a realm configuration file permits you to fine-tune retry policies for individual realms, and for specific targets within a realm. If you provide a [FastFail] section, the ProxyFastFail parameter in the radius.ini [Configuration] section is ignored.
Chapter 7: Realm Configuration Files

[ModifyUser] Section

The [ModifyUser] section of a realm configuration file permits you to decorate a realm, where the realm is determined by other means, such as DNIS or attribute mapping.

This is used mainly to enhance directed realms. For example, the following two users are in the database: george@gm and george@ford. Either user could log in as george, as Steel-Belted Radius would determine the realm, for example, by DNIS. Based on the realm, Steel-Belted Radius would append either @gm or @ford to the user name, and then use the Native User directed method to authenticate.

This methodology could also be used in a double-proxy situation. The first proxy uses DNIS to determine a realm, then decorates the name and forwards it to the next hop server. This second proxy (which may be a legacy RADIUS server that doesn’t understand DNIS) could then handle realms based on the name decoration.

Table 86: RealmName.pro [FastFail] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MinFailures = x</td>
<td>These parameters define a tolerance level for failures to reach a target server within a realm. Such “failures” are judged according to the</td>
</tr>
<tr>
<td>MinSeconds = y</td>
<td>NumAttempts and RequestTimeout settings that you defined in the [Auth] or [Acct] sections.</td>
</tr>
<tr>
<td></td>
<td>A target is presumed down once x consecutive failures have occurred and at least y seconds have elapsed.</td>
</tr>
<tr>
<td></td>
<td>Once a target is presumed down, Steel-Belted Radius directs proxy requests to another target in the same realm, if available. It does not wait</td>
</tr>
<tr>
<td></td>
<td>for responses from the failed target.</td>
</tr>
<tr>
<td></td>
<td>However, it sends strobe requests periodically to the failed target to detect when that server comes back up. Once a response is received to one</td>
</tr>
<tr>
<td></td>
<td>of these strobe requests, that server is no longer presumed down.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Strobe requests are sent to the “down” target server only if there are proxy requests addressed to its realm.</td>
</tr>
<tr>
<td>ResetSeconds = z</td>
<td>Once the realm’s tolerance level is exceeded, this parameter specifies how long a target may be presumed down.</td>
</tr>
<tr>
<td></td>
<td>The ResetSeconds value indicates the maximum number of seconds during which a server can be presumed down in the absence of strobe</td>
</tr>
<tr>
<td></td>
<td>requests. If z seconds elapse with no strobe requests sent to the down server, the server is reset to “up.”</td>
</tr>
<tr>
<td></td>
<td>The status of a target that is presumed down is reset to “up” when one of the following occurs:</td>
</tr>
<tr>
<td></td>
<td>■ A response to a strobe request is received from the server.</td>
</tr>
<tr>
<td></td>
<td>■ There has been no request sent to the server for z seconds.</td>
</tr>
</tbody>
</table>

[ModifyUser] Syntax

These parameters define the User-Name prefix and suffix.

Table 87: RealmName.pro [ModifyUser] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddPrefix = prefix</td>
<td>These parameters define the User-Name prefix and suffix.</td>
</tr>
<tr>
<td>AddSuffix = suffix</td>
<td></td>
</tr>
</tbody>
</table>
**[SpooledAccounting] Section**

Proxy spooling is configured within the [SpooledAccounting] section of a *RealmName*.pro file.

```
[SpooledAccounting]
Enable=1
RolloverSeconds=600
RolloverSize=1048576
Directory=\all_acct_data
RetryInterval=60
ShutdownDelay=20
```

Table 88: *RealmName*.pro [SpooledAccounting] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>■ If set to 1, proxy spooling is enabled. ■ If set to 0, proxy spooling is disabled. Default value is 0.</td>
</tr>
<tr>
<td>RolloverSeconds</td>
<td>Specifies the rollover interval in seconds. After the interval elapses, the current spool file is closed and a new one is created. Default value is 600 (10 minutes.)</td>
</tr>
<tr>
<td>RolloverSize</td>
<td>Specifies the rollover file size limit in bytes. After the file size exceeds this limit, the current spool file is closed and a new one is created. If both RolloverSeconds and RolloverSize are set, the first parameter that exceeds its limit initiates rollover. Default value is 1,048,576 bytes (1 megabyte).</td>
</tr>
</tbody>
</table>
| Directory         | Specifies the directory where the spool (.psf) files are stored. The directory must be manually created in the RADIUS service directory. Default value is \RealmName\  

**NOTE:** Each realm must have its own directory for spool files. Otherwise, packets for multiple realms would be interspersed and a problem in one realm could prevent subsequent packets to other realms from being forwarded.  

| RetryInterval     | Specifies the interval in seconds prior to retrying a proxy request if the target system (the downstream server where accounting data for this realm is sent) is down. Default value is 60. |
| ShutdownDelay     | Specifies the amount of time (given as the number of seconds) prior to the execution of a shutdown request during which the final undelivered spooled packets in the spool file can be sent to their target. This value should be set according to the amount of accounting data normally received for this realm, and other relevant network conditions.  

If the target system is down when Steel-Belted Radius shuts down, this setting is not applied, and unspooling terminates immediately (and Steel-Belted Radius shuts down immediately). Upon restart, unspooling of accounting data restarts from the beginning of the oldest spool file. Default value is 20.
NOTE: Do not enable proxy spooling for realms that are not enabled for accounting.

**Retry Sequence**

If Steel-Belted Radius receives an accounting packet for a realm, and the target system is down, Steel-Belted Radius implements the RealmName.pro retry configuration, as in the following example:

```
[Acct]
RequestTimeout=5, 3, 5
NumAttempts=3
```

In this example, Steel-Belted Radius attempts to proxy forward the accounting packet to the target IP address, as it would in a non-SpooledAccounting scenario. Three attempts are made; the first waits for five seconds before timing out, the second three seconds, and the third five seconds.

If there is still no response from the target after three attempts, the RetryInterval in the [SpooledAccounting] section is applied. If RetryInterval equals 60, then five seconds after the last unsuccessful NumAttempts is completed, Steel-Belted Radius waits another sixty seconds and then attempts the entire retry policy again.
**Directed Realm Configuration (.dir) File**

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM  
**Not used by:** EE

A directed realm specifies target methods for directed authentication and/or directed accounting. Its realm configuration file is called `RealmName.dir`. By default, an sample `.dir` file (`example.dir`) is installed with Steel-Belted Radius.

The directed authentication feature permits the server to bypass its Authentication Methods list and map an incoming RADIUS request to one or more specific authentication methods. Steel-Belted Radius chooses the destination method based on routing information found in the request packet. The destination methods may be any authentication methods already configured on the local Steel-Belted Radius server, regardless of how they were configured; for example, a method may have been configured using the Administrator windows, the LDAP configuration interface, or a `.aut` configuration file.

If no directed authentication method is configured, every request percolates through the same Authentication Methods list, as defined in the Authentication Policies panel in SBR Administrator. This behavior may or may not be ideal for every customer. Directed authentication lets you tailor an authentication methods list to a customer’s needs.

Directed accounting is also possible. The destination accounting method may be the Steel-Belted Radius accounting log, an external database configured using a `.acc` file, or a distinct accounting log file that contains entries only for this customer.

To activate these features, you must create `RealmName.dir` files, place them in the Steel-Belted Radius directory, and list them in the [Directed] section of `proxy.ini`. Subsequently, any requests that arrive addressed to one of these realm names are processed on the local server using the instructions you’ve provided in `proxy.ini` and in the corresponding `RealmName.dir` file.

After you edit a `RealmName.dir` file, you must apply your changes as follows. If you have added or changed:

- Any directed accounting methods, you must stop and restart the server to load your new configuration.
- Directed authentication methods in which external database (SQL or LDAP) authentication is used, you must stop and restart the server to load your new configuration.
- Directed authentication methods in which local or pass-through (Native, UNIX, Domain, Host, SecurID, or TACACS +) authentication is used, you can apply your configuration changes dynamically, without stopping the server.
  - **Solaris/Linux:** Issue the `HUP` signal to the Steel-Belted Radius process.  
    `kill -HUP ProcessID`
Windows: Run the RADHUP.EXE program from the command shell. (RADHUP.EXE is located in the server directory that you specified at installation time, usually C:\Program Files\Juniper Networks\Steel-Belted Radius\Service.)

Steel-Belted Radius re-reads proxy.ini, filter.ini, and all .pro and .dir files in the server directory, and resets its realm configuration accordingly.

**NOTE:** If you edit radius.ini while configuring a realm, you must restart Steel-Belted Radius to load your new configuration.

### [Auth] Section

Directed authentication is enabled in a realm by setting the Enable parameter in the [Auth] section of the corresponding RealmName.dir file, where RealmName is the name of the realm. The syntax is as follows:

```
[Auth]
Enable = 1
StripRealm = 1
UseMasterDictionary = yes
```

**Table 89: RealmName.dir [Auth] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Enable                | If set to 1 in the [Auth] section of a RealmName.dir file, the directed authentication realm called RealmName is enabled.  
  If set to 0, the realm is disabled.  
  By enabling a directed authentication realm, you make it possible for Steel-Belted Radius to override the Authentication Methods list on the local server by providing an alternate list - for requests addressed to this realm only. Details of this list are provided in the [AuthMethods] section of the same RealmName.dir file. |
| StripRealm            | If set to 1, Steel-Belted Radius strips the realm name from the username before attempting to authenticate the user's request.  
  If set to 0, realm name stripping is disabled.  
  **NOTE:** For directed realms, realm name is enabled (StripRealm = 1) by default. If you want to disable it, you must explicitly set StripRealm to 0. |
| UseMasterDictionary   | If set to yes, inbound proxy responses for this realm use the master Steel-Belted Radius dictionary when authentication attributes are filtered in.  
  If set to no, proxy responses for this realm use the client-specific dictionary when authentication attributes are filtered in.  
  Default value is yes.  
  **NOTE:** This value overrides the global setting configured in the UseMasterDictionary parameter in the proxy.ini file. |

### [AuthMethods] Section

If directed authentication is enabled, the [AuthMethods] section of a RealmName.dir file lists one or more authentication methods to be used.
The syntax is as follows:

```
[AuthMethods]
Description
Description
...
```

where `Description` is the “official name” of an authentication method configured on the Steel-Belted Radius server. For example:

```
[AuthMethods]
Native User
SecurID User
SecurID Prefix
SecurID Suffix
SecurID
TACACS+ User
TACACS+ Prefix
TACACS+ Suffix
Windows Domain User
Windows Domain Group
UNIX User
UNIX Group
<InitializationString=SQL>
<InitializationString=LDAP>
```

If you want your `[AuthMethods]` section to reference an external authentication method, a `Description` string must match the names of that method. If you want your `[AuthMethods]` section to reference an external database, enter the `InitializationString` value from the `[Bootstrap]` section of the corresponding `.aut` file.

---

**NOTE:** There is no interaction between the settings in the Authentication Policies panel and in `RealmName.dir` files, or between different `RealmName.dir` files. For example, if you disable the UNIX User method (for Solaris/Linux) or Windows Domain User method (for Windows) in the Authentication Policies panel while it is enabled in a `RealmName.dir` file, it remains enabled in `RealmName.dir`.

---

**[Acct] Section**

Directed accounting is enabled in a realm by setting the Enable parameter in the `[Acct]` section of the corresponding `RealmName.dir` file, where `RealmName` is the name of the realm. The syntax is as follows:

```
[Acct]
Enable = 1
StripRealm = 0
RecordLocally = 0
UseMasterDictionary = yes
```
Table 90: RealmName.dir [Acct] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>■ If set to 1 in the [Acct] section of a RealmName.dir file, the directed accounting realm called RealmName is enabled.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, the realm is disabled. By enabling a directed accounting realm, you make it possible for Steel-Belted Radius to override the normally configured accounting methods on the local server by providing an alternate list - for requests addressed to this realm only. Details of this list are provided in the [AcctMethods] section of the same RealmName.dir file. Default value is 0.</td>
</tr>
<tr>
<td>RecordLocally</td>
<td>■ If set to 1, Steel-Belted Radius writes accounting records to its main accounting log file in addition to the accounting destinations specified in [AcctMethods].</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, this feature is disabled. Default value is 0.</td>
</tr>
<tr>
<td>StaticAcctRealms</td>
<td>If a value is supplied for this parameter, accounting packets are forwarded to a list of realms. The setting given must be a section name defined in the proxyrl.ini file that lists the realms to which the accounting packets should be forwarded. See “Proxyrl.ini File” on page 163.</td>
</tr>
<tr>
<td>(GEE/SPE only)</td>
<td></td>
</tr>
<tr>
<td>StripRealm</td>
<td>■ If set to 1, Steel-Belted Radius strips the realm name from the username before attempting to authenticate the user’s request.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, realm name stripping is disabled.</td>
</tr>
<tr>
<td></td>
<td>NOTE: For directed realms, username stripping is enabled (StripRealm = 1) by default. If you want to disable it, you must explicitly set StripRealm to 0.</td>
</tr>
<tr>
<td>UseMasterDictionary</td>
<td>■ If set to yes, inbound proxy responses for this realm use the master Steel-Belted Radius dictionary when accounting attributes are filtered in.</td>
</tr>
<tr>
<td></td>
<td>■ If set to no, proxy responses for this realm use the client-specific dictionary when accounting attributes are filtered in.</td>
</tr>
<tr>
<td></td>
<td>Default value is yes.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This value overrides the global setting configured in the UseMasterDictionary parameter in the proxy.ini file.</td>
</tr>
</tbody>
</table>

[AcctMethods] Section

If directed accounting is enabled, the [AcctMethods] section of a RealmName.dir file lists one or more accounting methods to be used. The syntax is as follows:

```
[AcctMethods]
Description
Description
```

where Description is the “official name” of a directed accounting method configured in the proxy.ini file.
[Called-Station-ID] Section

The [Called-Station-ID] section of a RealmName.dir file allows Steel-Belted Radius to select a realm to be used for directed authentication and/or accounting based on DNIS information supplied in an incoming RADIUS packet. The [Called-Station-ID] section lists each DNIS string that identifies the realm. If this string is found in the Called-Station-Id attribute of an incoming request, the directed authentication and/or accounting rules found in the corresponding RealmName.dir file are applied to the request.

The syntax is as follows:

```
[Called-Station-ID]
  String
  String
  ...
```

where String is a DNIS string.

[ModifyUser] Section

The [ModifyUser] section of a realm directed file permits you to decorate a realm, where the realm is determined by other means, such as DNIS or attribute mapping.

This is used mainly to enhance directed realms. For example, the following two users are in the database: `george@gm` and `george@ford`. Either user could log in as `george`, as Steel-Belted Radius would determine the realm, for example, by DNIS. Based on the realm, Steel-Belted Radius would append either `@gm` or `@ford` to the user name, and then use the Native User directed method to authenticate.

Table 91: RealmName.dir [ModifyUser] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddPrefix = prefix</td>
<td>These parameters define the User-Name prefix and suffix.</td>
</tr>
<tr>
<td>AddSuffix = suffix</td>
<td></td>
</tr>
</tbody>
</table>
The `[Self]` section of `radius.ini` lets you list all of the realm names that should be handled by this Steel-Belted Radius server, rather than being proxied to other targets.

**GEE/SPE**: The `[Configuration]` section of `radius.ini` provides two parameters that you can use to enable or disable realm features for the Steel-Belted Radius server: ExtendedProxy and AttributeEdit. Both parameters are enabled (set to 1) by default. You can disable either feature by setting the corresponding parameter to 0.

**NOTE**: If you edit `radius.ini` while configuring a realm, you must stop and restart the Steel-Belted Radius server to load your new realm configuration.
radius.ini Realm Settings
Chapter 8

EAP Configuration Files

This chapter describes the EAP configuration and helper files, which specify options for automatic EAP helper methods. These files are loaded at startup time and resides in the Steel-Belted Radius directory.

<table>
<thead>
<tr>
<th>File</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>eap.ini File</td>
<td>184</td>
</tr>
<tr>
<td>fastauth.aut File</td>
<td>187</td>
</tr>
<tr>
<td>peapauth.aut File</td>
<td>193</td>
</tr>
<tr>
<td>tlsauth.aut File</td>
<td>199</td>
</tr>
<tr>
<td>tlsauth.eap File</td>
<td>206</td>
</tr>
<tr>
<td>ttlsauth.aut File</td>
<td>215</td>
</tr>
</tbody>
</table>
eap.ini File

**Used by:** GEE, SPE*, SPE + MIM*, SPE + EAP, EE

**Not used by:** —

You should use the SBR Administrator to maintain settings in the eap.ini file. You should not edit the eap.ini file manually.

The eap.ini configuration file configures the sequence in which EAP authentication types are tried when authenticating users by means of the different Steel-Belted Radius authentication methods.

Each authentication method that you want EAP authentication to be performed against must be configured within this eap.ini file.

This file must contain one section for each authentication method that you use, and the title of the section must identify the authentication method:

- Native User
- SecurID
- SecurID User
- SecurID Prefix
- SecurID Suffix
- LDAP
- SQL
- SQL-ORACLE
- Windows Domain User
- Windows Domain Group
- EAP-FAST
- EAP-TLS (GEE/EE/SPE + EAP)
- EAP-TTLS (GEE/EE/SPE + EAP)
- EAP-PEAP(GEE/EE/SPE + EAP)
- winauth
- defaultMethods

```
[Native-User]
EAP-Only = 0
First-Handle-Via-Auto-EAP = 0
EAP-Type = TTLS, LEAP, MD5-Challenge
Available-EAP-Types=MD5-Challenge,MS-CHAP-V2,LEAP,TLS
Available-EAP-Only-Values=0,1
Available-Auto-EAP-Values=1
```

**NOTE:** Steel-Belted Radius is configured with an eap.ini file that should work for most environments.
Table 92 lists the parameters in each section.

### Table 92: eap.ini Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| EAP-Only           | - If set to 0, the authentication method accepts all types of user credentials.  
                     | - If set to 1, the authentication method is given only EAP credentials or acts only as a back-end server to an automatic EAP protocol method.  
                     | For authentication methods expected to handle EAP-TTLS inner authentications, this parameter should be set to 0 or 1 depending on the type of credentials used in the inner authentication.  
                     | **NOTE:** If you are using SecurID with PEAP, set this value to 0. Since the PEAP plug-in converts the inner EAP/Generic Token credentials to PAP for security reasons, setting this value to 1 causes SecurID processing to be skipped when using EAP/Generic Token, ultimately leading to the user being rejected.  
| EAP-Type           | A comma-separated list of the EAP protocols to support for this authentication method. The first protocol in the list is the primary protocol. Protocols that appear later in the list are used with this authentication method only if the client responds with an EAP NAK and specifies such a protocol or if another authentication method triggers the use of the protocol but cannot complete the request. Valid values include the following:  
                     | - LEAP  
                     | - Generic-Token  
                     | - MD5-Challenge  
                     | - TTLS (GEE/EE only)  
                     | - TLS (GEE/EE only)  
                     | - MS-CHAP-V2 (GEE/EE only).  
                     | Leave the EAP-Type list empty to disable EAP for this authentication method.  
| First-Handle-Via-Auto-EAP | - If set to 1 and the user credentials are EAP, an appropriate automatic EAP helper method is called before the authentication method. The purpose of calling the automatic EAP helper method is to convert the user’s EAP credentials into a format acceptable to the authentication method.  
                     | - If set to 0, the authentication method itself handles the request directly, before any automatic helper methods.  
                     | Default varies based on type of user. Refer to the comments in the eap.ini file for more information.  
                     | **NOTE:** If you want to use machine authentication, you must enter 1 for this setting in the [Windows Domain User] and [Windows Domain Group] sections of eap.ini.  
                     | **NOTE:** You must set the AllowMachineLogin setting in the [WindowsDomain] section of winauth.aut to Yes if you want to use machine authentication. For more information, see “winauth.aut File” on page 106.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Available-EAP-Types        | A comma-separated list of the EAP protocols that can be selected when configuring the Steel-Belted Radius server by means of the SBR Administration. Valid values include the following:  
  - TTLS (GEE/EE only)  
  - TLS (GEE/EE only)  
  - MS-CHAP-V2 (GEE/EE only)  
  - FAST (GEE/EE only)  
  - LEAP  
  - Generic-Token  
  - MD5-Challenge  
| Available-EAP-Only-Values  | Controls whether the **Use EAP authentication only** checkbox in the EAP Setup window (accessed through the Authentication Policies panel in SBR Administrator) is enabled. Network administrators can use this parameter to control whether SBR Administrator users can select EAP authentication options.  
  - If set to 0,1, users can check and uncheck the **Use EAP authentication only** checkbox.  
  - If set to 0, the **Use EAP authentication only** option is disabled and the checkbox is inactive.  
  - If set to 1, the **Use EAP authentication only** option is enabled and the checkbox is inactive.  
| Available-Auto-EAP-Values  | Controls whether the **Handle via Auto-EAP first** checkbox in the EAP Setup window (accessed through the Authentication Policies panel in SBR Administrator) is enabled. Network administrators can use this parameter to control whether SBR Administrator users can select auto-EAP options.  
  - If set to 0,1, users can check and uncheck the **Handle via Auto-EAP first** checkbox.  
  - If set to 0, the **Handle via Auto-EAP first** option is disabled and the checkbox is inactive.  
  - If set to 1, the **Handle via Auto-EAP first** option is enabled and the checkbox is inactive.  
|                            | Default varies based on type of user. Refer to the comments in the **eap.ini** file for more information.
fastauth.aut File

**Used by:** GEE, SPE + EAP, EE  
**Not used by:** SPE, SPE + MIM

You should use the SBR Administrator to maintain settings in the fastauth.aut file. You should not edit the fastauth.aut file manually.

Settings for the EAP-FAST (Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling) authentication method are stored in the fastauth.aut file. The fastauth.aut configuration file is read each time the Steel-Belted Radius server restarts (or, if you are using the GEE or SPE edition of Steel-Belted Radius, each time the Steel-Belted Radius server receives a HUP signal).

### [Bootstrap] Section

The [Bootstrap] section of the fastauth.aut file (Table 93) specifies information that Steel-Belted Radius uses to load the EAP-FAST authentication method.

**Table 93: fastauth.aut [Bootstrap] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibraryName</td>
<td>Specifies the name of the EAP-FAST module. Default value is fastauth.dll for Windows and fastauth.so for Solaris and Linux. Do not change this unless you are advised to do so by Juniper Customer Support.</td>
</tr>
</tbody>
</table>
| Enable             | Specifies whether the EAP-FAST authentication module is enabled.  
|                    | - If set to 0, EAP-FAST is disabled, and the authentication method does not appear in the Authentication Methods list in the Authentication Policies panel.  
|                    | - If set to 1, EAP-FAST is enabled.  
|                    | Default value is 0.                                                        |
| InitializationString | Specifies the name of the authentication method to appear in the Authentication Methods list in the Authentication Policies panel.  
|                    | The name of each authentication method must be unique. If you create additional .aut files to implement authentication against multiple databases, the InitializationString value in each file must specify a unique method name.  
|                    | Default value is EAP-FAST.                                               |
The [Server_Settings] section (Table 94) lets you configure the basic operation of the EAP-FAST plug-in.

### Table 94: fastauth.aut [Server_Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_Message_Fragment_Length</td>
<td>Specifies the maximum size TLS message length that may be generated during each iteration of the TLS exchange. This value affects the number of RADIUS challenge/response round-trips required to conclude the TLS exchange. A value of 1400 may result in 6 round-trips, while a value of 500 may result in 15 round-trips. Some Access Points may have problems with RADIUS responses or EAP messages that exceed the size of one Ethernet frame (1500 bytes including IP/UDP headers). Minimum value is 500. Maximum value is 4096. Default value is 1020, which prevents the RADIUS challenge response (carried in a UDP packet) from exceeding one Ethernet frame.</td>
</tr>
<tr>
<td>Return_MPPE_Keys</td>
<td>Setting this attribute to 1 causes the module to include RADIUS MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes in the final RADIUS Accept response sent to the Access Point. This is necessary for the Access Point to key the WEP encryption. If the Access Point is authenticating only end-users and WEP is not being used, this attribute may be set to 0. Default value is 1.</td>
</tr>
<tr>
<td>DH_Prime_Bits</td>
<td>Specifies the size of the prime number that the module uses for Diffie-Hellman exponentiation. Selecting a larger prime number makes the system less susceptible to certain types of attacks but requires more CPU processing to compute the Diffie-Hellman key agreement operation. Valid values are 512, 1024, 1536, 2048, 3072, and 4096. Default value is 1024.</td>
</tr>
<tr>
<td>Cipher_Suites</td>
<td>Specifies the TLS cipher suites (in order of preference) that the server is to use. These cipher suites are documented in RFC 2246, “The TLS Protocol Version 1,” and other TLS-related RFCs and draft RFCs. Default value is: 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05, 0x04, 0x07, and 0x09.</td>
</tr>
<tr>
<td>Session_Timeout</td>
<td>If set to a number greater than 0, specifies the number of seconds a RADIUS client allows a session to persist before asking the client to re-authenticate. If set to 0, the Session-Timeout attribute is not generated. Default value is 0. <strong>NOTE:</strong> The RADIUS client must be configured to process the Session Timeout return attribute so that it can tell the client to reauthenticate after the session timer has expired.</td>
</tr>
</tbody>
</table>
Chapter 8: EAP Configuration Files

**[FAST_Protocol] Section**

The [FAST_Protocol] section lets you specify settings required by EAP-FAST. Table 95 describes the settings in the [FAST_Protocol] section of the fastauth.aut file.

**Table 95: fastauth.aut [FAST_Protocol] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Termination_Action</td>
<td>Specifies the value to return for the Termination-Action attribute sent in an accepted client. If no value is specified, the Termination-Action attribute is not sent.</td>
</tr>
<tr>
<td>Server_Secret_Lifetime_Days</td>
<td>Specifies the number of days that a server secret remains valid. A new server secret is created and stored by the EAP-FAST plug-in when the current secret expires. (Old secrets are retained until all PACs encrypted with the old secret have expired.) Server secrets are stored in the eapfast.info file. Default value is 30 days.</td>
</tr>
<tr>
<td>PAC_Lifetime_Days</td>
<td>Specifies the number of days provisioned PACs will be accepted. Default value is 90 days.</td>
</tr>
<tr>
<td>PAC_Reprovision_Days</td>
<td>Specifies the number of days before the expiration of a PAC that a new PAC should be provisioned. When a user presents a PAC that has less time to live than the reprovision time, a new PAC is provisioned using the existing PAC. Default value is 30 days.</td>
</tr>
<tr>
<td>Authority_Identifier_Info</td>
<td>Specifies the authority identifier that this server sends to users. The identity may be presented by client software to help select the appropriate PAC by the client.</td>
</tr>
<tr>
<td></td>
<td>■ If set to auto, the server identifies itself with the name of the server on which Steel-Belted Radius is installed.</td>
</tr>
<tr>
<td></td>
<td>■ If set to any other string, the server sends that string as the authority identifier.</td>
</tr>
<tr>
<td></td>
<td>Default value is auto.</td>
</tr>
</tbody>
</table>

**[Inner_Authentication] Section**

The [Inner_Authentication] section (Table 96) lets you specify the way in which the inner authentication step operates.

**Table 96: fastauth.aut [Inner_Authentication] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed_REALM</td>
<td>Omitting this setting causes the inner authentication request to be handled like any other request received from a RAS. Specifying the name of a directed realm causes the request to be routed based on the methods listed in the directed realm. Default is to process the inner authentication through standard request processing.</td>
</tr>
</tbody>
</table>
[Request Filters] Section

Request filters (Table 97) affect the attributes of inner authentication requests. By default, Steel-Belted Radius does not use request filters.

NOTE: The filters named in these settings must be defined in the `filter.ini` file.

Table 97: fastauth.aut [Request Filters] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Outer_Attribs_to_New</td>
<td>This filter affects only a new inner authentication request (rather than continuations of previous requests).</td>
</tr>
<tr>
<td></td>
<td>If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request.</td>
</tr>
<tr>
<td></td>
<td>If this filter is not specified, no attributes from the outer request are transferred to the inner request.</td>
</tr>
<tr>
<td>Transfer_Outer_Attribs_to_Continue</td>
<td>This filter affects only a continued inner authentication request (rather than the first inner authentication request).</td>
</tr>
<tr>
<td></td>
<td>If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request.</td>
</tr>
<tr>
<td></td>
<td>If this filter is not specified, no attributes from the outer request are transferred to the inner request.</td>
</tr>
<tr>
<td>Edit_New</td>
<td>This filter affects only a new inner authentication request (rather than continuations of previous requests).</td>
</tr>
<tr>
<td></td>
<td>If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_New in this table) and attributes included in the inner authentication request sent through the tunnel by the client.</td>
</tr>
<tr>
<td></td>
<td>If this filter is not specified, the request remains unaltered.</td>
</tr>
<tr>
<td>Edit_Continue</td>
<td>This filter affects only a continued inner authentication request (rather than a new inner authentication request).</td>
</tr>
<tr>
<td></td>
<td>If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_Continue in this table) and attributes included in the inner authentication request sent through the tunnel by the client.</td>
</tr>
<tr>
<td></td>
<td>If this filter is not specified, the request remains unaltered.</td>
</tr>
</tbody>
</table>

[Response Filters] Section

Response filters (Table 98) affect the attributes in the final response (Access-Accept or Access-Reject) returned to the originating RAS. By default, Steel-Belted Radius does not use response filters.

NOTE: The filters named in these settings must be defined in the `filter.ini` file.
Chapter 8: EAP Configuration Files

Example

[Bootstrap]
LibraryName=fastauth.dll
Enable=1
InitializationString=EAP-FAST

[Server_Settings]
; Indicates the maximum TLS Message fragment length EAP-TLS will handle. If not
; specified, this parameter defaults to 1020. It can be set as high as 4096,
; but sizes over 1400 bytes are likely to cause fragmentation of the UDP packet
; carrying the message and some RADIUS client may be incapable of dealing with
; this fragmentation.
TLS_Message_Fragment_Length = 1020

; Indicates whether or not the EAP-TLS module should return the
; MS-MPPE-Send-Key and MS-MPPE-Recv-Key attribute upon successfully
; authenticating the user. The default is to return these attributes.
Return_MPPE_Keys = 1

; Specifies the size of the prime to use for DH modular exponentiation. The
; choices are 512, 1024, 1536, 2048, 3072 and 4096. The default is 1024 bits.
DH_Prime_Bits = 1024

; Specifies the TLS cipher suites (in order of preference) that the server is
; to use. These cipher suites are documented in RFC 2246 and other TLS related
; RFCs or draft RFCs. The default is: 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05,
; 0x04, 0x07, 0x09
Cipher_Suites = 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05, 0x04, 0x07, 0x09

; Specifies the maximum length of time (in seconds) the RAS/AP will be
; instructed to allow the session to persist before the client is asked
; to re-authenticate. Specifying a 0 will cause the Session-Timeout attribute
; not to be generated by the plug-in. The default is 0.
; Session_Timeout = 0

Table 98: fastauth.aut [Response Filters] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Inner_Attribs_To_Accept</td>
<td>This filter affects only an outer Access-Accept response that is sent back to a network access device. If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response. If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.</td>
</tr>
<tr>
<td>Transfer_Inner_Attribs_To_Reject</td>
<td>This filter affects only an outer Access-Reject response that is sent back to a network access device. If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response. If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.</td>
</tr>
</tbody>
</table>
; Specifies the value to return for the Termination-Action attribute
; sent in an accepted client. If omitted in this file, the Termination-Action
; attribute will not be sent.
;Termination_Action =

[FAST_Protocol]
; Specifies the lifetime of a server secret in days. A new server secret is
; created and stored by the EAP-FAST plug-in when the current secret expires.
; The default is 30 days.
;Server_Secret_Lifetime_Days = 30

; Specifies the lifetime for provisioned PACs in days. This represents the time
; for which a provisioned PAC will be accepted. The default is 90 days.
PAC_Lifetime_Days = 90

; Specifies the policy on reprovisioning PACs. When a user presents a PAC that
; has less time to live than the reprovision time, a new PAC is provisioned
; using the existing PAC. The default is 30 days.
PAC_Reprovision_Days = 30

; Specifies the authority identifier that this server sends to clients. The
; identifier can be specified as ‘auto’, in which case the server will substitute
; the local host name, or as any other fixed string. The default is ‘auto’.
;Authority_Identifier_Info = auto

[Inner_Authentication]
; Specifies how inner authentication routing is to occur. You can choose to
; use the standard SBR routing logic (by omitting this attribute) or a directed
; realm. The default is to use the standard SBR routing logic.
;Directed_Realm = fast_realm

[Request_Filters]
; Specifies attribute filters to apply to the transfer of attributes from the
; outer to the inner authentication request (initial vs. continuations) and
; filters to apply after the inner authentication request attributes have been
; added to the request. These filters must be described in the filter.ini file.
; The default is not to use any filters.
;Transfer_Outer_Attribs_to_New = fast_transfer_outer_to_new
;Transfer_Outer_Attribs_to_Continue = fast_transfer_outer_to_continue
;Edit_New = fast_edit_new
;Edit_Continue = fast_edit_continue

[Response_Filters]
; Specifies attribute filters to the final response (accept or reject)
; received from SBR and forwarded to EAP-FAST originating RAS. These filters must
; be described in the filter.ini file. The default is not to use any filters.
;Transfer_Inner_Attribs_To_Accept = fast_transfer_inner_to_accept
;Transfer_Inner_Attribs_To_Reject = fast_transfer_inner_to_reject
peapauth.aut File

**Used by:** GEE, SPE + EAP, EE*
**Not used by:** SPE, SPE + MIM

You should use the SBR Administrator to maintain settings in the `peapauth.aut` file. You should not edit the `peapauth.aut` file manually.

Settings for the EAP-PEAP plug-in are stored in the `peapauth.aut` file. The `peapauth.aut` configuration file is read each time the Steel-Belted Radius server restarts (or, if you are using the GEE or SPE + EAP edition of Steel-Belted Radius, each time the Steel-Belted Radius server receives a HUP signal).

**[Bootstrap] Section**

The [Bootstrap] section of the `peapauth.aut` file (Table 99) specifies information that Steel-Belted Radius uses to load the EAP-PEAP authentication method.

### Table 99: `peapauth.aut` [Bootstrap] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibraryName</td>
<td>Specifies the name of the EAP-PEAP module. Default value is <code>peapauth.dll</code> for Windows and <code>peapauth.so</code> for Solaris and Linux. Do not change this unless you are advised to do so by Juniper Customer Support.</td>
</tr>
<tr>
<td>Enable</td>
<td>Specifies whether the EAP-PEAP authentication module is enabled.</td>
</tr>
<tr>
<td></td>
<td>- If set to 0, EAP-PEAP is disabled, and the authentication method does not appear in the Authentication Methods list in the Authentication Policies panel.</td>
</tr>
<tr>
<td></td>
<td>- If set to 1, EAP-PEAP is enabled. Default value is 0.</td>
</tr>
<tr>
<td>InitializationString</td>
<td>Specifies the name of the authentication method to appear in the Authentication Methods list in the Authentication Policies panel.</td>
</tr>
<tr>
<td></td>
<td>The name of each authentication method must be unique. If you create additional .aut files to implement authentication against multiple databases, the InitializationString value in each file must specify a unique method name.</td>
</tr>
<tr>
<td></td>
<td>Default value is EAP-PEAP.</td>
</tr>
</tbody>
</table>
**[Server_Settings] Section**

The [Server_Settings] section (Table 100) lets you configure the basic operation of the EAP-PEAP plug-in.

**Table 100: peapauth.aut [Server_Settings] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_Message_Fragment_Length</td>
<td>Set to the maximum size TLS message length that may be generated during each iteration of the TLS exchange. Some Access Points may have problems with RADIUS responses or EAP messages that exceed the size of one Ethernet frame (1500 bytes including IP/UDP headers). The default value (1020) prevents the RADIUS challenge response (carried in a UDP packet) from exceeding one Ethernet frame. This is likely to be the safest setting. Setting a smaller value affects the number of RADIUS challenge/response round-trips required to conclude the TLS exchange. While a value of 1400 may result in 6 round-trips, a value of 500 may result in 15 round-trips. The minimum value is 500.</td>
</tr>
<tr>
<td>Return_MPPE_Keys</td>
<td>Setting this attribute to 1 causes the module to include RADIUS MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes in the final RADIUS Accept response sent to the Access Point. This is necessary for the Access Point to key the WEP encryption. If the Access Point is authenticating only end-users and WEP is not being used, this attribute may be set to 0. Default value is 1.</td>
</tr>
<tr>
<td>DH_Prime_Bits</td>
<td>Specifies the size of the prime number that the module uses for Diffie-Hellman exponentiation. Selecting a larger prime number makes the system less susceptible to certain types of attacks but requires more CPU processing to compute the Diffie-Hellman key agreement operation. Valid values are 512, 1024, 1536, 2048, 3072, and 4096. Default value is 1024.</td>
</tr>
<tr>
<td>Cipher_Suites</td>
<td>Specifies the TLS cipher suites (in order of preference) that the server is to use. These cipher suites are documented in RFC 2246, “The TLS Protocol Version 1,” and other TLS-related RFCs and draft RFCs. Default value is: 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05, 0x04, 0x07, and 0x09.</td>
</tr>
<tr>
<td>PEAP_Min_Version</td>
<td>Specifies the minimum version of the PEAP protocol that the server should negotiate: If set to 0, the server negotiates version 0, which is compatible with Microsoft’s initial PEAP implementation (shipped in Microsoft XP Service Pack 1). If set to 1, the server negotiates version 1, which is compatible with Cisco’s initial PEAP implementation (shipped in Cisco ACU). Default value is 0. NOTE: The value entered in this setting must be less than or equal to the value entered for the PEAP_Max_Version setting.</td>
</tr>
</tbody>
</table>
Chapter 8: EAP Configuration Files

[Inner_Authentication] Section

Used by: GEE, SPE + EAP
Not used by: SPE, SPE + MIM, EE

The [Inner_Authentication] section (Table 101) lets you specify the way in which the inner authentication step is to operate.

Table 101: peapauth.aut [Inner_Authentication] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed_Realm</td>
<td>Omitting this setting causes the inner authentication request to be handled like any other request received from a RAS. Specifying the name of a directed realm causes the request to be routed based on the methods listed in the directed realm. Default is to process the inner authentication through standard request processing.</td>
</tr>
</tbody>
</table>

NOTE: The value entered in this parameter must be equal to or greater than the value entered for PEAP_Min_Version.

[Request Filters] Section

Request filters (Table 102) affect the attributes of inner authentication requests.

Table 102: peapauth.aut [Request Filters] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Outer_Attribs_to_New</td>
<td>This filter affects only a new inner authentication request (rather than continuations of previous requests). If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request. If this filter is not specified, no attributes from the outer request are transferred to the inner request.</td>
</tr>
</tbody>
</table>

NOTE: The filters named in these settings must be defined in the filter.ini file.
Table 102: peapauth.aut [Request Filters] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Outer_Attribs_to_Continue</td>
<td>This filter affects only a continued inner authentication request (rather than the first inner authentication request).&lt;br&gt; If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request.&lt;br&gt; If this filter is not specified, no attributes from the outer request are transferred to the inner request.</td>
</tr>
<tr>
<td>Edit_New</td>
<td>This filter affects only a new inner authentication request (rather than continuations of previous requests).&lt;br&gt; If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_New in this table) and attributes included in the inner authentication request sent through the tunnel by the client.&lt;br&gt; If this filter is not specified, the request remains unaltered.</td>
</tr>
<tr>
<td>Edit_Continue</td>
<td>This filter affects only a continued inner authentication request (rather than a new inner authentication request).&lt;br&gt; If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_Continue in this table) and attributes included in the inner authentication request sent through the tunnel by the client.&lt;br&gt; If this filter is not specified, the request remains unaltered.</td>
</tr>
</tbody>
</table>

**NOTE:** The filters named in these settings must be defined in the filter.ini file.

[Response Filters] Section

Response filters (Table 103) affect the attributes in the responses returned to authentication requests.

Table 103: peapauth.aut [Response Filters] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Inner_Attribs_To_Accept</td>
<td>This filter affects only an outer Access-Accept response that is sent back to a network access device.&lt;br&gt; If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response.&lt;br&gt; If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.</td>
</tr>
</tbody>
</table>
Chapter 8: EAP Configuration Files

Table 103: peapauth.aut [Response Filters] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Inner_Attribs_To_Reject</td>
<td>This filter affects only an outer Access-Reject response that is sent back to a network access device. If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response. If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.</td>
</tr>
</tbody>
</table>

**NOTE:** The filters named in these settings must be defined in the filter.ini file.

[Session_Resumption] Section

The [Session_Resumption] section (Table 104) lets you specify whether session resumption is permitted and under what conditions session resumption is performed.

**NOTE:** For session resumption to work, the network access device must be configured to handle the Session-Timeout return list attribute, because the network access device must be able to tell the client to reauthenticate after the session timer has expired.

Table 104: peapauth.aut [Session_Resumption] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session_Timeout</td>
<td>Set this attribute to the maximum number of seconds you want the client to remain connected to the network access device before having to re-authenticate.</td>
</tr>
<tr>
<td></td>
<td>- If set to a number greater than 0, the lesser of this value and the remaining resumption limit (see description below) is sent in a Session-Limit attribute to the RADIUS client on the RADIUS Access Accept response.</td>
</tr>
<tr>
<td></td>
<td>- If set to 0, no Session-Limit attribute is generated by the plug-in. This does not prevent the authentication methods performing secondary authorization from providing a value for this attribute.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td>Entering a value such as 600 (10 minutes) does not necessarily cause a full re-authentication to occur every 10 minutes. You can configure the resumption limit to make most re-authentications fast and computationally cheap.</td>
</tr>
</tbody>
</table>
Termination_Action Set this attribute to the integer value that you want returned in a Termination-Action attribute. This is a standard attribute supported by most Access Points and determines what happens when the session timeout is reached.

If you do not specify a value for this attribute, the plug-in does not generate such an attribute. This does not prevent the authentication methods performing secondary authorization from providing a value for this attribute.

Default is to not send this attribute.

Resumption_Limit Set this attribute to the maximum number of seconds you want the client to be able to re-authenticate using the TLS session resumption feature.

This type of re-authentication is fast and computationally cheap. It does, however, depend on previous authentications and may not be considered as secure as a complete (computationally expensive) authentication. Specifying a value of 0 disables the session resumption feature.

Default value is 0.
**tlsauth.aut File**

**Used by:** GEE, SPE + EAP, EE  
**Not used by:** SPE, SPE + MIM

You should use the SBR Administrator to maintain settings in the tlsauth.aut file. You should not edit the tlsauth.aut file manually.

Settings for the EAP-TLS authentication method are stored in the tlsauth.aut file. The tlsauth.aut configuration file is read each time the Steel-Belted Radius server restarts (or, if you are using the GEE or SPE + EAP edition of Steel-Belted Radius, each time the Steel-Belted Radius server receives a HUP signal).

**[Server_Settings] Section**

The [Server_Settings] section contains the settings that control the basic operation of the EAP-TLS authentication method.

**Table 105: tlsauth.aut [Server_Settings] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_Message_Fragment_Length</td>
<td>Maximum TLS message length that may be generated during each iteration of the TLS exchange. Anecdotal evidence suggests that some Access Points may have problems with RADIUS responses or EAP messages that exceed the size of one Ethernet frame (1500 bytes including IP/UDP headers). The default value (1020) prevents the RADIUS challenge response (carried in a UDP packet) from exceeding one Ethernet frame. This is likely to be the safest setting. Setting a smaller value affects the number of RADIUS challenge/response round-trips required to conclude the TLS exchange. While a value of 1400 may result in 6 round-trips, a value of 500 may result in 15 round-trips. The minimum value is 500.</td>
</tr>
</tbody>
</table>
Verify_User_Name_Is_Principal_Name

Certificates issued by Microsoft’s Windows 2000 Certificate Server typically include a Subject Alternative Name/Other Name attribute, where Principal Name set to something like user@certtest.acme.com.

The Windows XP client that supports EAP-TLS in conjunction with 802.1X extracts this attribute value from the client’s certificate and uses it to respond to the Access Point’s EAP Identity Request. The Access Point, in turn, packages up this value as the RADIUS User-Name attribute in requests it sends to a RADIUS server.

- If set to 1, the EAP-TLS module verifies that the contents of the RADIUS User-Name attribute match the ‘Principal Name’ of the certificate used to authenticate the user.

- If set to 0, no such check is performed. The value should be set to 0 if the certificates used do not include a ‘Principal Name’ or if the client being used does not report the contents of ‘Principal Name’ as the user’s identity in response to an EAP Identity Request.

Default value is 0.

Return_MPPE_Keys

Setting this attribute to 1 causes the EAP-TLS module to include RADIUS MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes in the final RADIUS Accept response sent to the Access Point. This is necessary for the Access Point to key the WEP encryption. If the Access Point is authenticating only end-users and WEP is not being used, this attribute may be set to 0.

Default value is 1.

DH_Prime_Bits

Specifies the size of the prime number that the module uses for Diffie-Hellman exponentiation. Selecting a larger prime number makes the system less susceptible to certain types of attacks but requires more CPU processing to compute the Diffie-Hellman key agreement operation.

Valid values are 512, 1024, 1536, 2048, 3072, and 4096.

Default value is 1024.

Cipher_Suites

Specifies the TLS cipher suites (in order of preference) that the server is to use. These cipher suites are documented in RFC 2246, “The TLS Protocol Version 1,” and other TLS-related RFCs and draft RFCs.

Default value is: 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05, 0x04, 0x07, and 0x09.

Profile

Specifies a profile that is to be used to select attributes sent back on an Access-Accept.

By default, additional attributes are not sent back.
[CRL_Checking] Section

The [CRL_Checking] section (Table 106) lets you specify settings that control how Steel-Belted Radius performs certificate revocation list (CRL) checking.

Table 106: tlsauth.aut [CRL_Checking] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Specifies whether CRL checking is enabled. Default value is 0 (disabled).</td>
</tr>
<tr>
<td>Retrieval_Timeout</td>
<td>Specifies the time (in seconds) that EAP-TLS will wait for a CRL checking transaction to complete when the CRL check involves a CRL retrieval. When CRL retrieval takes longer than the specified time, the user’s authentication request will result in a reject. Default value is 5 seconds.</td>
</tr>
<tr>
<td>Expiration_Grace_Period</td>
<td>Specifies the time (in seconds) after expiration during which a CRL is still considered acceptable. EAP-TLS will always attempt to retrieve a new CRL when it is presented with a certificate chain and it finds an expired CRL in its cache.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0 (strict expiration mode), EAP-TLS will not accept a CRL that has expired.</td>
</tr>
<tr>
<td></td>
<td>■ If set to a value greater than 0 (lax expiration mode), EAP-TLS will consider the expired CRL as an acceptable stand-in from the time the CRL expires to the time the grace period ends.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0 (strict expiration mode).</td>
</tr>
<tr>
<td>Allow_Missing_CDP_Attribute</td>
<td>Specifies whether the omission of a CDP attribute in a non-root certificate is acceptable. Without a CDP attribute, EAP-TLS will not know how to retrieve a CRL and will not be able to perform a revocation check on the certificate.</td>
</tr>
<tr>
<td></td>
<td>■ If set to false, EAP-TLS will not accept a CRL with a missing CDP attribute.</td>
</tr>
<tr>
<td></td>
<td>■ If set to true, EAP-TLS will allow such certificates and skip CRL checking for them.</td>
</tr>
<tr>
<td></td>
<td>Default value is true.</td>
</tr>
<tr>
<td>Default_LDAP_Server_Name</td>
<td>Specifies what LDAP server name to use if the CDP contains a value that begins with the string <code>/ldap:\\</code>. This style of CDP (generated by some CAs) does not include the identity of the LDAP server. Specify the name of the LDAP that contains the CRLs if you expect to encounter certificates with this style CDP. If you don’t specify a server name and such certificates are encountered, the CRL retrieval will fail.</td>
</tr>
</tbody>
</table>
[Session_Resumption] Section

The [Session_Resumption] section (Table 107) lets you specify whether session resumption is permitted and under what conditions session resumption is performed.

NOTE: For session resumption to work, the network access device must be configured to handle the Session-Timeout return list attribute, because the network access device must be able to tell the client to reauthenticate after the session timer has expired.

Table 107: tlsauth.aut [Session_Resumption] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Session_Timeout | Set this attribute to the maximum number of seconds you want the client to remain connected to the network access device before having to re-authenticate.  
If set to a number greater than 0, the lesser of this value and the remaining resumption limit (see description below) is sent in a Session-Limit attribute to the RADIUS client on the RADIUS Access Accept response.  
If set to 0, no Session-Limit attribute is generated by the plug-in. Note that this does not prevent the authentication methods performing secondary authorization from providing a value for this attribute.  
Default value is 0.  
Entering a value such as 600 (10 minutes) does not necessarily cause a full re-authentication to occur every 10 minutes. You can configure the resumption limit to make most re-authorizations fast and computationally cheap. |
| Termination_Action | Set this attribute to the integer value that you want returned in a Termination-Action attribute. This is a standard attribute supported by most Access Points and determines what happens when the session timeout has been reached.  
If you do not specify a value for this attribute, the plug-in does not generate such an attribute. This does not prevent the authentication methods performing secondary authorization from providing a value for this attribute.  
Default value is 0 (“Do not to send this attribute”). |
| Resumption_Limit | Set this attribute to the maximum number of seconds you want the client to be able to re-authenticate using the TLS session resumption feature.  
This type of re-authentication is fast and computationally cheap. It does, however, depend on previous authentications and may not be considered as secure as a complete (computationally expensive) authentication. Specifying a value of 0 disables the session resumption feature.  
Default value is 0. |
Sample tlsauth.aut File

[Bootstrap]
LibraryName=tlsauth.dll
Enable=0
InitializationString=EAP-TLS

[Server_Settings]
; Note that all trusted root certificates
; must have a .der file extension and
; must be placed in the ROOT directory
; immediately below the directory
; containing the SBR 'radius' daemon and
; the radius.ini file.

; Indicates the maximum TLS Message fragment
; length EAP-TLS will handle. If not
; specified, this parameter defaults to 1020.
; It can be set as high as 4096,
; but sizes over 1400 bytes are likely to cause
; fragmentation of the UDP packet
; carrying the message and some RADIUS client
; may be incapable of dealing with
; this fragmentation.
;TLS_Message_Fragment_Length = 1020

; Indicates whether or not the EAP-TLS module
; it to check whether the User Name
; provided in the RADIUS request matches the
; principal name in the client's
; certificate. The default is not to perform
; this check.
;Verify_User_Name_Is_Principal_Name = 0

; Indicates whether or not the EAP-TLS module
; should return the
; MS-MPPE-Send-Key and MS-MPPE-Recv-Key
; attribute upon successfully
; authenticating the user. The default is
; to return these attributes.
;Return_MPPE_Keys = 1

; Specifies the size of the prime to use
; for DH modular exponentiation. The
; choices are 512, 1024, 1536, 2048, 3072
; and 4096. The default is 1024 bits.
;DH_Prime_Bits = 1024

; Specifies the TLS cipher suites (in order
; of preference) that the server is
; to use. These cipher suites are documented
; in RFC 2246 and other TLS related
; RFCs or draft RFCs. The default is: 0x16, 0x13,
; 0x66, 0x15, 0x12, 0xa0, 0x05, 0x04, 0x07, 0x09
;Cipher_Suites = 0x16, 0x13, 0x66, 0x15, 0x12, 0xa0, 0x05, 0x04, 0x07, 0x09

; Specifies a profile that is to be used
; to select attributes sent back on an
; Access-Accept. The default is not to send
; any additional attributes.
; Profile = <profile-name>

[CRL_Checking]
; Specifies whether CRL checking is to be enabled.
; The default is to disable CRL checking.
; Enable = 0

; Specifies the time (in seconds) that EAP-TLS
; will wait for a CRL checking
; transaction to complete when the CRL check
; involves a CRL retrieval. When
; CRL retrieval takes longer than the
; specified time, the user’s authentication
; request will result in a reject. The
; default value is 5 seconds.
; Retrieval_Timeout = 5

; Specifies the time (in seconds) after
; expiration during which a CRL is
; still considered acceptable. EAP-TLS will
; always attempt to retrieve a
; new CRL when it is presented with a
; certificate chain and it finds an
; expired CRL in its cache. EAP-TLS
; will consider the expired CRL as an
; acceptable stand-in from the time the
; CRL expires to the time the grace
; period ends.
; Expiration_Grace_Period = 0

; Specifies whether the omission of a
; CDP attribute in a non-root certificate
; is acceptable. Without a CDP attribute,
; EAP-TLS will not know where to
; retrieve a CRL from and will not be
; able to perform a revocation check on
; the certificate. The default is allow
; such certificates and to skip CRL
; checking for them.
; Allow_Missing_CDP_Attribute = 1

; Specifies what LDAP server name to
; use if the CDP contains a value that
; begins with the string "/\ldap:\\\".
; This style of CDP (generated by some
; CAs does not include the identity of
; the LDAP server. Specify the name of
; the LDAP that contains the CRLs if you
; expect to encounter certificates
; with this style CDP if you don’t specify
; a server name and such certificates
; are encountered, the CRL retrieval will fail.
; Default_LDAP_Server_Name = <hostname>
[Session_Resumption]
; Specifies the maximum length of time (in seconds)
; the RAS/AP will be
; instructed to allow the session to persist
; before the client is asked
; to re-authenticate. Specifying a 0 will
; cause the Session-Timeout attribute
; not to be generated by the plug-in. The default is 0.
;Session_Timeout = 0

; Specifies the value to return for the
; Termination-Action attribute
; sent in an accepted client. If omitted in
; this file, the Termination-Action
; attribute will not be sent.
Termination_Action = 0

; Specifies the length of time (in seconds)
; during which an authentication
; request that seeks to resume a previous TLS
; session will be considered
; acceptable. Specifying 0 will cause session
; resumption support to be
; disabled. The default is 0.
Resumption_Limit = 3600
## tlsauth.eap File

**Used by:** GEE, SPE + EAP, EE  
**Not used by:** SPE, SPE + MIM

You should use the SBR Administrator to maintain settings in the tlsauth.eap file. You should not edit the tlsauth.eap file manually.

Settings for the EAP-TLS automatic EAP helper are stored in the tlsauth.eap file. The tlsauth.eap configuration file is read each time the Steel-Belted Radius server restarts (or, if you are using the GEE or SPE edition of Steel-Belted Radius, each time the Steel-Belted Radius server receives a HUP signal).

### [Server_Settings] Section

The [Server_Settings] section (Table 108) contains the settings that control the basic operation of the EAP-TLS authentication process.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_Message_Fragment_Length</td>
<td>Maximum TLS message length that may be generated during each iteration of the TLS exchange. Anecdotal evidence suggests that some Access Points may have problems with RADIUS responses or EAP messages that exceed the size of one Ethernet frame (1500 bytes including IP/UDP headers). The default value (1020) prevents the RADIUS challenge response (carried in a UDP packet) from exceeding one Ethernet frame. This is likely to be the safest setting. Setting a smaller value affects the number of RADIUS challenge/response round-trips required to conclude the TLS exchange. While a value of 1400 may result in 6 round-trips, a value of 500 may result in 15 round-trips. The minimum value is 500.</td>
</tr>
</tbody>
</table>
Table 108:  tlsauth.eap [Server_Settings] Syntax  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify_User_Name_Is_Principal_Name</td>
<td>Certificates issued by Microsoft's Windows 2000 Certificate Server usually include a Subject Alternative Name/Other Name attribute, where Principal Name set to something like <a href="mailto:user@certtest.acme.com">user@certtest.acme.com</a>. The MS Windows XP client that supports EAP-TLS in conjunction with 802.1X extracts this attribute value from the client’s certificate and uses it to respond to the Access Point’s EAP Identity Request. The Access Point, in turn, packages up this value as the RADIUS User-Name attribute in requests it sends to a RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>▪ If set to 1, the EAP-TLS module verifies that the contents of the RADIUS User-Name attribute match the 'Principal Name' of the certificate used to authenticate the user.</td>
</tr>
<tr>
<td></td>
<td>▪ If set to 0, no such check is performed. The value should be set to 0 if the certificates used do not include a 'Principal Name' or if the client being used does not report the contents of 'Principal Name' as the user's identity in response to an EAP Identity Request.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>Return_MPPE_Keys</td>
<td>Setting this attribute to 1 causes the EAP-TLS module to include RADIUS MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes in the final RADIUS Accept response sent to the Access Point. This is necessary for the Access Point to key the WEP encryption. If the Access Point is authenticating only end-users and WEP is not being used, this attribute may be set to 0.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1.</td>
</tr>
<tr>
<td>DH_Prime_Bits</td>
<td>Specifies the size of the prime number that the module uses for Diffie-Hellman exponentiation. Selecting a larger prime number makes the system less susceptible to certain types of attacks but requires more CPU processing to compute the Diffie-Hellman key agreement operation.</td>
</tr>
<tr>
<td></td>
<td>Valid values are 512, 1024, 1536, 2048, 3072, and 4096.</td>
</tr>
<tr>
<td></td>
<td>Default value is 1024.</td>
</tr>
<tr>
<td>Cipher_Suites</td>
<td>Specifies the TLS cipher suites (in order of preference) that the server is to use. These cipher suites are documented in RFC 2246, “The TLS Protocol Version 1,” and other TLS-related RFCs and draft RFCs.</td>
</tr>
<tr>
<td></td>
<td>Default value is: 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05, 0x04, 0x07, and 0x09.</td>
</tr>
</tbody>
</table>
[Secondary_Authorization] Section

The [Secondary_Authorization] section lets you specify whether secondary authorization is performed and, if it is, what information is used in the secondary authorization request.

Table 109: tlsauth.eap [Secondary_Authorization] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Specifies whether secondary authorization checking is enabled.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, this feature is disabled and the EAP-TLS plug-in accepts the user upon proof of ownership of a private key that matches a valid certificate. If this setting is 0, no other settings in this section are applicable to the plug-in’s operation.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, a secondary authorization check against a traditional authentication method such as an SQL plug-in is performed. Default value is 1.</td>
</tr>
<tr>
<td>Convert_User_Name_To_Subject_CN</td>
<td>Once the EAP-TLS module has concluded its processing, it may still defer to a traditional authentication method (core or plug-in) for final authorization. To do so, it must provide a user name and password to the traditional authentication method.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, the EAP-TLS module parses the Subject attribute of the client’s certificate for the least significant ‘CN = ’ and takes the value of this attribute (for example, ‘George Washington’) as the user name being passed to the traditional authentication method.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> Convert_User_Name_To_Subject_CN and Convert_User_Name_To_Principal_Name cannot both be set to 0 and cannot both be set to 1. Default value is 1.</td>
</tr>
<tr>
<td>Convert_User_Name_To_Principal_Name</td>
<td>Once the EAP-TLS module has concluded its processing, it may still defer to a traditional authentication method (core or plug-in) for final authorization. To do so, it must provide a user name and password to the traditional authentication method.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, the user name passed to the traditional authentication method is the user name retrieved from the Subject field of the client certificate (see description of Convert_User_Name_To_Subject_CN above).</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, the EAP-TLS module uses the principal name (Subject Alternate Name or Other Name) from the client certificate (for example, ‘<a href="mailto:joe@acme.com">joe@acme.com</a>’) as the user name being passed to the traditional authentication method.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> Convert_User_Name_To_Subject_CN and Convert_User_Name_To_Principal_Name cannot both be set to 0 and cannot both be set to 1.</td>
</tr>
</tbody>
</table>
Chapter 8: EAP Configuration Files

[Session_Resumption] Section

The [Session_Resumption] section lets you specify whether session resumption is permitted and under what conditions session resumption is performed. The [Session_Resumption] section consists of the parameters listed in Table 109.

Table 109: tlsauth.eap [Secondary_Authorization] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>FixedPassword</td>
<td>By default, the secondary authorization check includes a user name but no other user credentials, because no password or similar credential for the client is available at the conclusion of the TLS handshake. Some authentication methods (Native User, LDAP, and SQL) can be configured to not require user credentials. If you plan to use secondary authorization against an authentication method (for example, LDAP) that cannot be configured to ignore the lack of user credentials, you may specify a fixed password that the plug-in uses on all secondary authorization checks. Default is to perform the check without user credentials.</td>
</tr>
</tbody>
</table>
| Include_Certificate_Info   | If set to 1, the EAP-TLS plug-in adds four attributes to the request before the secondary authorization check is performed:  
  - The Funk-Peer-Cert-Subject attribute contains the value of the Subject attribute in the client certificate.  
  - The Funk-Peer-Cert-Principal attribute contains the value of the principal name (Subject Alternate Name or Other Name) attribute of the client certificate.  
  - The Funk-Peer-Cert-Issuer attribute contains the value of the Issuer attribute in the client certificate.  
  - The Funk-Peer-Cert-Hash attribute contains a hexadecimal ASCII representation of the SHA1 hash of the client certificate.  
These attributes are ignored if the authentication method that will perform the authentication check does not use them. Default value is 0. |

NOTE: For session resumption to work, the network access device must be configured to handle the Session-Timeout return list attribute, because the network access device must be able to tell the client to reauthenticate after the session timer has expired.
Sample tlsauth.eap File

[Bootstrap]
LibraryName=tlauth.dll
Enable=1

; Maximum TLS Message fragment length
TLS_Message_Fragment_Length = 1020

; Indicates whether the EAP-TLS module is to check
; whether the User Name provided in the RADIUS request
; matches the principal name in the client’s certificate.
Verify_User_Name_Is_Principal_Name = 1

; Indicates whether the EAP-TLS module should return
; the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attribute upon
; successfully authenticating the user.
Return_MPPE_Keys = 1
; Specifies the size of the prime to use for DH modular
; exponentiation.
DH_Prime_Bits = 1536

[Secondary_Authorization]
; Indicates whether secondary authorization is to be
; performed. Set to 1 to require a secondary authorization
; check against traditional authentication method
; (for example, SQL plug-in)
Enable = 1

; Indicates whether the plug-in should substitute the CN
; contained in the client certificate for the RADIUS User
; Name before the secondary authorization check
Convert_User_Name_To_Subject_CN = 1

; Indicates whether the plug-in should substitute the
; principal name contained in the Subject Alternate Name
; (Other Name) field of the client certificate for the
; RADIUS User Name before secondary authorization check.
Convert_User_Name_To_Principal_Name = 0

; Indicates whether the secondary authorization check
; should use no user credentials or a fixed password.
FixedPassword = test

; Indicates whether attributes containing information
; about the client certificate should be added to the
; request before secondary authorization is performed.
; The attributes include Funk-Peer-Cert-Subject,
; Funk-Peer-Cert-Principal, Funk-Peer-Cert-Issuer, and
; Funk-Peer-Cert-Hash. The default is not to include
; these attributes.
Include_Certificate_Info = 0

[Session_Resumption]
; Maximum length of time (in seconds) the RAS/AP will
; allow the session to persist before the client is asked
; to re-authenticate.
Session_Timeout = 600

; The value to return for the Termination-Action attribute
; sent in an accepted client.
Termination_Action = 0

; The length of time (in seconds) during which an
; authentication request that seeks to resume a previous
; TLS session will be considered acceptable.
Resumption_Limit = 3600
**Configuring Secondary Authorization**

The EAP-TLS plug-in may be configured to perform a secondary authorization check that typically requires a traditional authentication method that can be configured to authenticate users without the presence of credentials.

Examples for the Oracle SQL plug-in, the LDAP plug-in, and Native User authentication are provided below.

**SQL Authentication**

The .aut file below shows an example of how the Oracle SQL plug-in on Solaris/Linux can be configured so that password information is not required as input or output.

To configure these two plug-ins to cooperate, no password has been given in the SQL= string entry in the [Settings] section, and the Password= entry in the [Results] section has been similarly left empty.

```
[Bootstrap]
LibraryName=radsql_auth_ora.so
Enable=1
InitializationString=Oracle SQL Auth

[Settings]
; OracleInstance is database instance, ($ORACLE_SID from shell)
Connect=OracleUser/OraclePassword@OracleInstance

; Other than procedures, non-interactive SQL statements are not
; terminated
SQL=SELECT FullName FROM orasqlauth WHERE username = %Name/50s
ParameterMarker=?
MaxConcurrent=1
ConcurrentTimeout=10
ConnectTimeout=10
QueryTimeout=10
WaitReconnect=2
MaxWaitReconnect=15

; LogLevel and TraceLevel for this plugin, regardless of radius.ini
LogLevel=0
TraceLevel=0

[Results]
; Empty definition of Password= indicates password to be ignored,
; since EAP-TLS is assumed to have already authenticated the user.
Password=
FullName=1/255s
;Profile=2/48
;Alias=3/48

[Failure]
;Accept=0
;Profile=xyz
;FullName=Remote User
```
Chapter 8: EAP Configuration Files

If the SQL authentication method used for secondary authorization is intended to be used only in conjunction with EAP-TLS, use SBR Administrator to set `EAP-Only=1` and `EAP-Type=TLS` in the appropriate section of the `eap.ini` file to prevent unintended use of this SQL authentication method for traditional authentication requests.

**LDAP Authentication**

The `.aut` file below shows an example of how the LDAP plug-in can be configured so that password information is not required as input or output.

To configure the EAP-TLS and LDAP plug-ins to cooperate properly, the `BindName=` option has been utilized in the [Settings] section to log into the LDAP server and no `%password=` setting has been specified in the [Response] section.

```
[Settings]
MaxConcurrent=2
Timeout=20
ConnectTimeout=5
QueryTimeout=10
WaitReconnect=2
MaxWaitReconnect=30
BindName=uid=admin,ou=administrators,o=bigco.com
Bindpassword=adminPassword
LogLevel=2
UpperCaseName=0
PasswordCase=original
Search=DoLdapSearch
SSL=0

[Server]
s1=

[Server/s1]
Host=199.185.162.147
Port=389

[Request]
%Username=User-Name

[Response]
%profile=TheUserProfile

[Search/DoLdapSearch]
Base=ou=Special Users,o=bigco.com
Scope=2
Filter=(uid=<User-Name>)
Attributes=AttrList
Timeout=20
%DN=dn

[Attributes/AttrList]
userprofile
```

If the LDAP authentication method used for secondary authorization is intended to be used only in conjunction with EAP-TLS, use SBR Administrator to set `EAP-Only=1` and `EAP-Type=TLS` in the appropriate section of the `eap.ini` file to prevent unintended use of this LDAP authentication method for traditional authentication requests.
Native User Authentication

The only requirement for using EAP-TLS in conjunction with Native User authentication is that appropriate values must be set in SBR Administrator for the First-Handle-Via-Auto-EAP and EAP-Type settings in the eap.ini file.
**ttlsauth.aut File**

*Used by:* GEE, SPE + EAP, EE*

*Not used by:* SPE, SPE + MIM

You should use the SBR Administrator to maintain settings in the `ttlsauth.aut` file. You should not edit the `ttlsauth.aut` file manually.

Settings for the EAP-TTLS authentication method are stored in the `ttlsauth.aut` file. The `ttlsauth.aut` configuration file is read each time the Steel-Belted Radius server restarts (or, if you are using the GEE or SPE edition of Steel-Belted Radius, each time the Steel-Belted Radius server receives a HUP signal).

**[Bootstrap] Section**

The [Bootstrap] section of the `ttlsauth.aut` file (Table 111) specifies information that Steel-Belted Radius uses to load the EAP-TTLS authentication method.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibraryName</td>
<td>Specifies the name of the EAP-TTLS module. Default value is <code>ttlsauth.dll</code> for Windows and <code>ttlsauth.so</code> for Solaris and Linux. Do not change this unless you are advised to do so by Juniper Customer Support.</td>
</tr>
<tr>
<td>Enable</td>
<td>Specifies whether the EAP-TTLS authentication module is enabled.</td>
</tr>
<tr>
<td>InitializationString</td>
<td>Specifies the name of the authentication method to appear in the Authentication Methods list in the Authentication Policies panel. The name of each authentication method must be unique. If you create additional .aut files to implement authentication against multiple databases, the InitializationString value in each file must specify a unique method name. Default value is EAP-TTLS.</td>
</tr>
</tbody>
</table>

**[Server_Settings] Section**

The [Server_Settings] section (Table 112) lets you configure the basic operation of the EAP-TTLS plug-in.
Table 112: ttlsauth.aut [Server_Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_Message_Fragment_Length</td>
<td>Specifies the maximum size TTLS message length that may be generated during each iteration of the TTLS exchange. This value affects the number of RADIUS challenge/response round-trips required to conclude the TTLS exchange. A value of 1400 may result in 6 round-trips, while a value of 500 may result in 15 round-trips. Some Access Points may have problems with RADIUS responses or EAP messages that exceed the size of one Ethernet frame (1500 bytes including IP/UDP headers). Minimum value is 500. Maximum value is 4096. Default value is 1020, which prevents the RADIUS challenge response (carried in a UDP packet) from exceeding one Ethernet frame.</td>
</tr>
<tr>
<td>Return_MPPE_Keys</td>
<td>Setting this attribute to 1 causes the module to include RADIUS MS-MPPE-Send-Key and MS-MPPE-Recv-Key attributes in the final RADIUS Accept response sent to the Access Point. This is necessary for the Access Point to key the WEP encryption. If the Access Point is authenticating only end-users and WEP is not being used, this attribute may be set to 0. Default value is 1.</td>
</tr>
<tr>
<td>DH_Prime_Bits</td>
<td>Specifies the size of the prime number that the module uses for Diffie-Hellman exponentiation. Selecting a larger prime number makes the system less susceptible to certain types of attacks but requires more CPU processing to compute the Diffie-Hellman key agreement operation. Valid values are 512, 1024, 1536, 2048, 3072, and 4096. Default value is 1024.</td>
</tr>
<tr>
<td>Cipher_Suites</td>
<td>Specifies the TLS cipher suites (in order of preference) that the server is to use. These cipher suites are documented in RFC 2246, “The TLS Protocol Version 1,” and other TLS-related RFCs and draft RFCs. Default value is: 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05, 0x04, 0x07, and 0x09.</td>
</tr>
<tr>
<td>Require_Client_Certificate</td>
<td>■ If set to 1, specifies that the client must provide a certificate as part of the TTLS exchange. ■ If set to 0, no client certificate is required. Default value is 0.</td>
</tr>
</tbody>
</table>

[Inner_Authentication] Section

**Used by:** GEE, SPE + EAP  
**Not used by:** SPE, SPE + MIM, EE

The [Inner_Authentication] section (Table 113) lets you specify the way in which the inner authentication step is to operate.
Chapter 8: EAP Configuration Files

Table 113: ttlsauth.aut [Inner_Authentication] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed_Realm</td>
<td>Omitting this setting causes the inner authentication request to be handled like any other request received from a RAS. Specifying the name of a directed realm causes the request to be routed based on the methods listed in the directed realm. Default is to process the inner authentication through standard request processing.</td>
</tr>
</tbody>
</table>

[Request Filters] Section

Request filters (Table 114) affect the attributes of inner authentication requests.

NOTE: The filters named in these settings must be defined in the filter.ini file.

Table 114: ttlsauth.aut [Request Filters] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Outer_Attribs_to_New</td>
<td>This filter affects only a new inner authentication request (rather than continuations of previous requests). If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request. If this filter is not specified, no attributes from the outer request are transferred to the inner request.</td>
</tr>
<tr>
<td>Transfer_Outer_Attribs_to_Continue</td>
<td>This filter affects only a continued inner authentication request (rather than the first inner authentication request). If this filter is specified, all attributes from the outer request are transferred to the inner request and this filter is applied. The transfer occurs and the filter is applied before any attributes specified in the inner authentication are added to the request. If this filter is not specified, no attributes from the outer request are transferred to the inner request.</td>
</tr>
<tr>
<td>Edit_New</td>
<td>This filter affects only a new inner authentication request (rather than continuations of previous requests). If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_New in this table) and attributes included in the inner authentication request sent through the tunnel by the client. If this filter is not specified, the request remains unaltered.</td>
</tr>
</tbody>
</table>
Table 114: ttlsauth.aut [Request Filters] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit_Continue</td>
<td>This filter affects only a continued inner authentication request (rather than a new inner authentication request). If this filter is specified, it is applied to the inner request that is the cumulative result of attributes transferred from the outer request (see Transfer_Outer_Attribs_To_Continue in this table) and attributes included in the inner authentication request sent through the tunnel by the client. If this filter is not specified, the request remains unaltered.</td>
</tr>
</tbody>
</table>

[Response Filters] Section

Response filters (Table 115) affect the attributes in the responses returned to authentication requests.

NOTE: The filters named in these settings must be defined in the filter.ini file.

Table 115: ttlsauth.aut [Response Filters] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transfer_Inner_Attribs_To_Accept</td>
<td>This filter affects only an outer Access-Accept response that is sent back to a network access device. If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response. If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.</td>
</tr>
<tr>
<td>Transfer_Inner_Attribs_To_Reject</td>
<td>This filter affects only an outer Access-Reject response that is sent back to a network access device. If this filter is specified, the filter is applied to the inner authentication response and all resulting attributes are transferred to the outer authentication response. If this filter is not specified, no inner authentication response attributes are transferred to the outer authentication response.</td>
</tr>
</tbody>
</table>

[CRL_Checking] Section

The [CRL_Checking] section (Table 116) lets you specify settings that control how Steel-Belted Radius performs certificate revocation list (CRL) checking.

Table 116: ttlsauth.aut [CRL_Checking] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>If set to 1, specifies that CRL checking is enabled for EAP-TTLS. Default value is 0.</td>
</tr>
</tbody>
</table>
### Table 116: ttlsauth.aut [CRL_Checking] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieval_Timeout</td>
<td>Specifies the time (in seconds) that EAP-TTLS waits for a CRL checking transaction to complete when the CRL check involves a CRL retrieval. When CRL retrieval takes longer than the specified time, the user’s authentication request is rejected. Default value is 5 seconds.</td>
</tr>
</tbody>
</table>
| Expiration_Grace_Period       | Specifies the time (in seconds) after expiration during which a CRL is still considered acceptable. EAP-TTLS always attempts to retrieve a new CRL when it is presented with a certificate chain and it finds an expired CRL in its cache.  
- If set to 0 (strict expiration mode), EAP-TTLS does not accept a CRL that has expired.  
- If set to a value greater than 0 (lax expiration mode), EAP-TTLS considers the expired CRL as an acceptable stand-in from the time the CRL expires to the time the grace period ends. Default value is 0 (strict expiration mode). |
| Allow_Missing_CDP_Attribute   | Specifies whether the omission of a CDP attribute in a non-root certificate is acceptable. Without a CDP attribute, EAP-TLS does not know how to retrieve a CRL and cannot perform a revocation check on the certificate.  
- If set to 0, EAP-TLS does not accept a CRL with a missing CDP attribute.  
- If set to 1, EAP-TLS allows such certificates and skips CRL checking for them. Default value is 1. |
| Default_LDAP_Server_Name      | Specifies what LDAP server name to use if the CDP contains a value that begins with the string //ldap:/. This style of CDP (generated by some CAs) does not include the identity of the LDAP server. Specify the name of the LDAP that contains the CRLs if you expect to encounter certificates with this style CDP. If you don’t specify a server name and such certificates are encountered, CRL retrieval fails. |

### [Session_Resumption] Section

The [Session_Resumption] section (Table 117) lets you specify whether session resumption is permitted and under what conditions session resumption is performed.

**NOTE:** For session resumption to work, the network access device must be configured to handle the Session-Timeout return list attribute, because the network access device must be able to tell the client to reauthenticate after the session timer has expired.
The [Integrity_Settings] section (Table 118) specifies the list of quarantine profiles that can be used by the optional Endpoint Assurance Server software to specify how to process users designated for isolation.

[Integrity_Settings]

;Quarantine_Profiles=QUARANTINE QUARANTINE2

### Table 117: ttlsauth.aut [Session_Resumption] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session_Timeout</td>
<td>Set this attribute to the maximum number of seconds you want the client to remain connected to the network access device before having to re-authenticate.</td>
</tr>
<tr>
<td></td>
<td>- If set to a number greater than 0, the lesser of this value and the remaining resumption limit (see description below) is sent in a Session-Limit attribute to the network access device on the RADIUS Access Accept response.</td>
</tr>
<tr>
<td></td>
<td>- If set to 0, no Session-Limit attribute is generated by the plug-in. This does not prevent the authentication methods performing secondary authorization from providing a value for this attribute.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td>Entering a value such as 600 (10 minutes) does not necessarily cause a full re-authentication to occur every 10 minutes. You can configure the resumption limit to make most re-authentications fast and computationally cheap.</td>
</tr>
<tr>
<td>Termination_Action</td>
<td>Set this attribute to the integer value that you want returned in a Termination-Action attribute. This is a standard attribute supported by most Access Points and determines what happens when the session timeout is reached.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a value for this attribute, the plug-in does not generate such an attribute. This does not prevent the authentication methods performing secondary authorization from providing a value for this attribute.</td>
</tr>
<tr>
<td></td>
<td>Default is to not send this attribute.</td>
</tr>
<tr>
<td>Resumption_Limit</td>
<td>Set this attribute to the maximum number of seconds you want the client to be able to re-authenticate using the TLS session resumption feature.</td>
</tr>
<tr>
<td></td>
<td>This type of re-authentication is fast and computationally cheap. It does, however, depend on previous authentications and may not be considered as secure as a complete (computationally expensive) authentication. Specifying a value of 0 disables the session resumption feature.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
</tbody>
</table>
Table 118: ttlsauth.aut [Integrity_Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine_Profiles</td>
<td>Identifies the list of Steel-Belted Radius profiles that can be assigned to users designated for isolation by the Endpoint Assurance Server software. To enter more than one profile name, enter each name on the same line, separating the profile names with a space. Default value is no quarantine profiles.</td>
</tr>
</tbody>
</table>

Sample ttlsauth.aut File

[Bootstrap]
LibraryName=ttlsauth.dll
Enable=1
InitializationString=EAP-TTLS

; Maximum TLS Message fragment length EAP-TLS will handle.
TLS_Message_Fragment_Length = 1020

; Indicates whether the EAP-TLS module should return the MS-MPPE-Send-Key and MS-MPPE-Recv-Key attribute upon successful authentication of user.
Return_MPPE_Keys = 1

; Size of the prime to use for DH modular exponentiation.
DH_Prime_Bits = 1536

; TLS cipher suites (in order of preference) that the server is to use.
Cipher_Suites = 0x16, 0x13, 0x66, 0x15, 0x12, 0x0a, 0x05, 0x04, 0x07, 0x09

GEE/SPE+EAP only

[Inner_Authentication]
; Specifies how inner authentication routing operates.
Directed_Realm = ttls_realms

[Request_Filters]
Transfer_Outer_Attribs_to_New = My_Xfer_Out_New_Filter
Transfer_Outer_Attribs_to_Continue = My_Xfer_Out_Continue_Filter
Edit_New = My_Edit_New_Filter
Edit_Continue = My_Continue_Filter

[Response_Filters]
Transfer_Inner_Attribs_To_Accept = My_Xfer_Acc_Filter
Transfer_Inner_Attribs_To_Reject = My_Xfer_Rej_Filter

[Session_Resumption]
; Maximum length of time (in seconds) the RAS/AP will allow the session to persist before the client is asked to re-authenticate.
Session_Timeout = 600

; Value to return for the Termination-Action attribute sent
; sent in an accepted client.
Termination_Action = 0

; Maximum length of time (in seconds) during which an authentication
; request that seeks to resume a previous TLS session will be
; considered acceptable.
Resumption_Limit = 3600

[Integrity_Settings]
; Specifies the list of valid quarantine profiles, which can be used
; by the Endpoint Assurance Server to specify isolated access.
; The default is no valid quarantine profiles.
;Quarantine_Profiles=QUARANTINE

For this to work, you must also provide the following settings in the [EAP-TTLS]
section of the eap.ini file:

    First-Handle-Via-Auto-EAP = 0
    EAP-Type = TTLS
Chapter 9

SNMP Configuration Files

This chapter describes how to configure and use the optional Simple Network Management Protocol (SNMP) package to monitor your Steel-Belted Radius server.

**NOTE:** SNMP is supported on the GEE and SPE editions of Steel-Belted Radius running on Solaris and Linux servers. SNMP is not supported on any edition of Steel-Belted Radius running on a Windows server.

<table>
<thead>
<tr>
<th>File</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>jnprsnmpd.conf</td>
<td>224</td>
</tr>
<tr>
<td>testagent.sh</td>
<td>230</td>
</tr>
</tbody>
</table>
The `jnprsnmpd.conf` configuration file stores settings for the SNMP agent. After you install the SNMP agent for Steel-Belted Radius on a Solaris or Linux server, you can modify the `jnprsnmpd.conf` configuration file to reflect your network environment.

**Access Control Section**

The `com2sec` keyword maps each source/community pair to a security name. The `com2sec` entry is used to determine a security name from the traditional community string, taking into account where a request has come from.

The syntax for the `com2sec` keyword is:

```
com2sec security_name source community
```

where:

- `security_name` identifies the security name you want to create.
- `source` can be a hostname, a subnet, or the word `default`. You can specify a subnet as an IP address and mask (`nnn.nnn.nnn.nnn/nnn.nnn.nnn.nnn`) or as an IP address and Classless Inter-Domain Routing (CIDR) bits (`nnn.nnn.nnn.nnn/nn`).
- `community` is an SNMP community string, which acts as a password to authenticate SNMP communications.

**NOTE:** If you use a CIDR address to identify a subnet, the host portion of the CIDR address must be 0. For example, if you are using the equivalent of a Class C subnet such as 192.168.1.x, you must enter the network address as 192.168.1.0/24 (which is the equivalent of 192.168.1.0/255.255.255.0).

The first source/community combination that matches an incoming packet is selected.

For example, the following creates two security names (`local` and `mynetwork`) and maps them to two different subnet/community name pairs.

<table>
<thead>
<tr>
<th>com2sec</th>
<th>sec.name</th>
<th>source</th>
<th>community</th>
</tr>
</thead>
<tbody>
<tr>
<td>com2sec</td>
<td>local</td>
<td>localhost</td>
<td>remote_community</td>
</tr>
<tr>
<td></td>
<td>mynetwork</td>
<td>192.168.1.0/24</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** When you install Steel-Belted Radius, you are prompted to enter your SNMP settings by the installation script. The installation script updates the `jnprsnmpd.conf` file based on the values you enter.
Security Names Section

The `group` keyword maps security names into group names. The `group` keyword gives general control by mapping between a security name (for a particular protocol version), and the internal name used in the access line.

The syntax for the `group` keyword is:

```
group name model security
```

where:

- `name` is the name of an access group.
- `model` identifies the security model you want to use: v1 or v2c.
- `security` is a security name.

For example, the following maps the two security names to four group/model pairs.

```
#     sec.model  sec.name
group LocalGroup  v1    local
group LocalGroup  v2c   local
group LANGroup    v1    mynetwork
group LANGroup    v2c   mynetwork
```

Access View Section

The `view` keyword specifies what portions of the MIB tree a specified group can view or modify. The syntax for the `view` keyword is:

```
view name {include | excluded} subtree mask
```

where:

- `name` is the identifier used for the view.
- `include/excluded` lets you include or exclude specific portions of the MIB tree from the view.
- `subtree` identifies the portion of the MIB tree that this name refers to in numeric or named form.
- `mask` specifies what elements of the MIB subtree should be regarded as relevant. When the entire MIB can be viewed, you can omit the mask field.

Group Access Section

The `access` keyword to specify who has access to part or all of the MIB tree. The syntax for the `access` keyword is:

```
access name context model level prefix read write notify
```

where:

- `name` is the name of a group.
`context` specifies the context for the view. For SNMPv1 or SNMPv2c, `context` should be empty.

`model` is the security model: any, v1, or v2c.

`level` can be used to ensure that the request is authenticated or encrypted. For SNMPv1 or SNMPv2c, `level` should be `noauth`.

`prefix` specifies how the `context` setting should be matched against the context of the incoming PDU. Enter `exact` or `prefix`.

`read` specifies the view to be used for READ access.

`write` specifies the view to be used for WRITE access.

`notify` specifies the view to be used for NOTIFY access.

For example, the following specifies that the LocalGroup uses the all view for READ, WRITE, and NOTIFY access.

```
# context model level prefix read write notify
access LocalGroup "" any noauth exact all all all
access LANGroup "" any noauth exact all none none
```

**System Contact Section**

You can specify your system contact information in the `jnprsnmpd.conf` file or in the MIB. If you configure your system contact information in the `jnprsnmpd.conf` file, the objects are locked and cannot be modified by means of SNMP.

System contact information consists of the following:

- `syslocation` – The physical location of the managed device.
- `syscontact` – The person or department responsible for maintaining the managed device.
- `sysname` – The name of the managed device.

This information is stored in the system group of the MIB-II tree.

The syntax for specifying system contact information is:

```
syslocation string
syscontact string
sysname string
```

**Traps Section**

Traps can be used by network entities to signal abnormal conditions to management stations. You should identify the NMS that receives trap messages generated by the Steel-Belted Radius server.
**NOTE:** You can configure Steel-Belted Radius to use either SNMPv1 or SNMPv2c traps. You cannot configure Steel-Belted Radius to generate both types of traps simultaneously.

- The `trapcommunity` keyword specifies the default community string to be used when sending traps.
  
  Syntax for the `trapcommunity` keyword is:
  ```
  trapcommunity string
  ```
  The `trapcommunity` keyword must precede the `trap2sink` keyword in the `jnprsnmpd.conf` file.

- The `trapsink` and `trap2sink` keywords specify whether you want Steel-Belted Radius to use either SNMPv1 traps or SNMPv2c traps. Do not enable both types of traps at the same time.
  
  - The `trapsink` keyword specifies the host or hosts to which the Steel-Belted Radius server should send SNMPv1 trap messages.
    
    Syntax for the `trapsink` keyword is:
    ```
    trapsink host [community [port]]
    ```
    where:
    - `host` specifies the host name or IP address of the NMS.
    - `community` specifies the community string the NMS expects.
    - `port` specifies the port on which the NMS is listening for SNMPv1 trap messages.

    For example:
    ```
    # send v1 traps
    trapsink nms.system.com secret
    ```

  - The `trap2sink` keyword specifies the host or hosts to which the Steel-Belted Radius server should send SNMPv2c trap (notification) messages.
    
    Syntax for the `trap2sink` keyword is:
    ```
    trap2sink host [community [port]]
    ```
    where:
    - `host` specifies the host name or IP address of the NMS.
    - `community` specifies the community string the NMS expects.
    - `port` specifies the port on which the NMS is listening for SNMPv2c trap messages.
For example:

```
# send v2 traps
trap2sink nms.system.com secret
```

## SNMP Proxy Section

The optional `proxy` keyword configures the SNMP agent to forward incoming SNMP requests to another agent.

Syntax for the `proxy` keyword is:

```
proxy [SNMPCMD ARGS] HOST OID [REMO TEDOID]
```

where: SNMPCMD keyword and arguments indicate how to authenticate the proxy SNMP.

### Table 119: SNMPCMD Keywords

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-c community</code></td>
<td>Set the community string for SNMP v1/v2c transactions.</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Dump the sent and received SNMP packets in hexadecimal format.</td>
</tr>
<tr>
<td><code>-r retries</code></td>
<td>Specifies the number of retries to be used in the request. Default value is 5.</td>
</tr>
<tr>
<td><code>-t timeout</code></td>
<td>Specifies the number of seconds between retries. Default value is 1.</td>
</tr>
<tr>
<td>`-v {1</td>
<td>2c</td>
</tr>
</tbody>
</table>

## [snmp] Section

The SNMP agent uses the `jnprsnmpd.conf` file to store static agent configuration information, such as community strings. The SNMP agent uses the `persist` directory to store information set during the running of the agent, which needs to be persistent from one run to the next.

The `persistentDir` keyword in the `[snmp]` section of `jnprsnmpd.conf` specifies the location of the `persist` directory. By default, the `persist` directory is located in the `radiusdir\snmp` directory on your server.

The syntax for specifying the location of the `persist` directory is as follows:

```
[snmp]
persistentDir radiusdir/snmp/persist
```

## [snmpd] Section

By default, `jnprsnmpd` listens for incoming SNMP requests on UDP port 161 on all IP interfaces. You can specify a different UDP port in the `jnprsnmpd.conf` file. The syntax for specifying a listening port is as follows:

```
[snmpd]
agentaddress port_number
```
Chapter 9: SNMP Configuration Files

Subagent Section

By default, the SNMP subagent in Steel-Belted Radius communicates with the SNMP agent on a configurable TCP port. The `sbr_admin_parameters` keyword specifies host, port, and interval values.

Syntax for the `sbr_admin_parameters` keyword is:

```
# sbr_admin_parameters host=localhost port=port tryinterval=interval
```

where:

- `port` identifies the TCP port the Steel-Belted Radius server uses for SNMP subagent-agent communication. The default value is TCP port 6669.

- `interval` specifies the number of seconds information can remain in the SNMP subagent cache. If your SNMP management station will issue queries intermittently, set the `tryinterval` value to a small number (1-5) to ensure timely information. If your SNMP management station will poll the server periodically, set the `tryinterval` value to a larger number to avoid flooding the server with queries. The default is 10 seconds.

radiusdir Section

The `sbr_private_directory` keyword specifies the location where Steel-Belted Radius is stored on your server.

Syntax for the `sbr_private_directory` keyword is:

```
sbr_private_directory radiusdir
```

The Steel-Belted Radius installer overwrites `radiusdir` with the appropriate value for your system. You should not need to change this value.

---

**NOTE:** If you change the SNMP port number in `jnprsnmpd.conf`, you must also enter the same port number in `testagent.sh`.

---

**NOTE:** If you run more than one SNMP agent on your server, each agent must use a unique UDP port number.
testagent.sh

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM  
**Not used by:** EE

You can run the `testagent.sh` script to verify that the jnprsnmpd SNMP agent is functioning. Before you do so, you must configure the `testagent.sh` file with the community string for your network.

The syntax for the `testagent.sh` file is as follows:

```bash
snmpget_path -M mib_directory -c community port sysDescr
```

### Table 120: testagent.sh Syntax

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmpget_path</code></td>
<td>Specifies the path for the <code>snmpget</code> utility.</td>
</tr>
<tr>
<td><code>-M mib_directory</code></td>
<td>Specifies the directory for the MIBs used by the SNMP agent.</td>
</tr>
<tr>
<td><code>-c community</code></td>
<td>Specifies the community string for your network.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>Specifies the default port for SNMP traffic.</td>
</tr>
<tr>
<td><code>sysDescr</code></td>
<td>Specifies the MIB variable to be retrieved.</td>
</tr>
</tbody>
</table>

*Default values:*  
- `snmpget_path`: `radiusdir/snmp/bin/snmpget`  
- `mib_directory`: `/radiusdir/snmp/mibs`  
- `community`: `COMMUNITY`  
- `port`: `localhost:161`  
- `sysDescr`: `system.sysDescr.0`
Chapter 10

SQL Authentication Files

This chapter describes the files used to configure SQL authentication in Steel-Belted Radius.
SQL Authentication Header Files

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM, EE*
**Not Used By:** —

The header files used to configure SQL authentication methods must have the .aut extension; for example, sqlauth.aut. The format of a header file is comparable to that of a Windows INI file: it is composed of several sections; section names are enclosed in brackets; each section may contain multiple parameter/value pairs.

**[Bootstrap] Section**

The [Bootstrap] section of the SQL authentication header file (Table 121) specifies information that Steel-Belted Radius uses to load and start an SQL authentication method.

```
[Bootstrap]
  LibraryName=sqauth.dll
  Enable=0
  InitializationString=SQL
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibraryName</td>
<td>Specifies the name of the SQL authentication module.</td>
</tr>
<tr>
<td></td>
<td>* Enter radsql_auth_ora.so for Oracle on Solaris.</td>
</tr>
<tr>
<td></td>
<td>* Enter radsql_auth_jdbc.so for JDBC on Solaris or Linux.</td>
</tr>
<tr>
<td></td>
<td>* Enter SQLAUTH.DLL for SQL on Windows.</td>
</tr>
<tr>
<td>Enable</td>
<td>Specifies whether the SQL authentication method is enabled.</td>
</tr>
<tr>
<td></td>
<td>* If set to 0, the authentication method is disabled and does not appear</td>
</tr>
<tr>
<td></td>
<td>in the Authentication Methods list in the Authentication Policies panel.</td>
</tr>
<tr>
<td></td>
<td>* If set to 1, the authentication method is enabled.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>InitializationString</td>
<td>Specifies the name of the authentication method to appear in the</td>
</tr>
<tr>
<td></td>
<td>Authentication Methods list in the Authentication Policies panel.</td>
</tr>
<tr>
<td></td>
<td>In the sample header file, this entry is set to SQL. You can modify</td>
</tr>
<tr>
<td></td>
<td>this name as needed.</td>
</tr>
<tr>
<td></td>
<td>The name of each authentication method must be unique. If you create</td>
</tr>
<tr>
<td></td>
<td>additional .aut files to implement authentication against multiple</td>
</tr>
<tr>
<td></td>
<td>databases, the InitializationString value in each file must specify a</td>
</tr>
<tr>
<td></td>
<td>unique method name.</td>
</tr>
</tbody>
</table>

**[FailedSuccessResultAttributes] Section**

The [FailedSuccessResultAttributes] section of the SQL authentication header file (Table 122) can be used to map any RADIUS attribute returned from the database. Attributes can be specified in two ways:

- Attributes can be specified with a literal value enclosed in single quotes. Values must be enclosed with single quotes, even when they represent numeric values.
Attributes can be specified with a numeric value that corresponds to the ordering of values returned from the SQL `select` statement.

Precede attribute names with `@` and enter them as they appear in the dictionary (.dct) files. Enclose attribute values (including integers and IP addresses) in single quotes. For example:

```
[FailedSuccessResultAttributes]
@Reply-Message = 'Please re-enter your password.'
@Filter-Id = '3'
```

**[Failure] Section**

**Used by:** GEE, SPE, SPE+EAP, SPE+MIM  
**Not used by:** EE

The [Failure] section of the SQL authentication header file can be used to determine the result of the authentication process (accept or reject) when connectivity to all of the configured SQL databases has failed. For example:

```
[Failure]
Accept = 1
Profile = XYZ
FullName = Unauthenticated!
```

**NOTE:** The Profile option and the Alias option cannot be used together. Read the following descriptions and choose the one that suits your needs.

<table>
<thead>
<tr>
<th>Table 122: *.aut [Failure] Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
</tbody>
</table>
| Accept | • If set to 1, Steel-Belted Radius returns an Access-Accept packet with the Profile, FullName, and/or Alias attributes specified in the corresponding [Failure] section parameters.  
• If set to 0, the user is rejected.  
Profile | Specifies the name of a Steel-Belted Radius profile whose checklist and return list attributes are applied to the user’s connection.  
FullName | By indicating a FullName, Steel-Belted Radius returns a value in the class attribute, allowing for all [Failure] connections to be accounted. |
### [Results] Section

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM, EE*

**Not used by:** —

The [Results] section of the SQL authentication header file maps the columns named in its SELECT query to the type of data that Steel-Belted Radius expects these columns to contain.

```plaintext
[Results]
Password=1/48
Profile=2/48
```

The following parameters may be present in a [Results] section. Each parameter represents a type of data required to authenticate an Access-Request, and if desired, apply authorization information as well.

**NOTE:** The Profile option and the Alias option cannot be used together. Read the following descriptions and choose the one that suits your needs.

### Table 123: *.aut [Results] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>%Password</td>
<td>The value returned from this column is understood to be the user’s password. The value returned by the SQL query is then matched with the user’s password received in the Access-Request. By default, Steel-Belted Radius expects the user’s password to stored in the SQL table in clear text format. If you want to configure Steel-Belted Radius to expect that the password value is encrypted with UNIXcrypt, then set PasswordFormat to 3 in the [Settings] section of the SQL authentication header file.</td>
</tr>
</tbody>
</table>
Consider the following `SELECT` statement:

```
SELECT user_pwd, attribs, fullname FROM rasusers WHERE user_id = %name
```

Table 123: *.aut [Results] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%Profile</code></td>
<td>The value returned from this column is interpreted as the name of the profile to associate with the user. The value returned by the SQL query is matched with an existing Profile entry of the same name. If the value is <code>prof1</code>, and a Profile called <code>prof1</code> exists in the Steel-Belted Radius database, any return list or checklist attributes in <code>prof1</code> are applied to the user’s connection. If the value cannot be matched with an existing Profile in the Steel-Belted Radius database, the user is rejected due to “Insufficient Resources.”</td>
</tr>
<tr>
<td><code>%ProxyRealm</code></td>
<td>Specifies the realm to which the authentication must be proxied. If ProxyRealm is not set, Routed Proxy does not occur.</td>
</tr>
<tr>
<td><code>%ProxyUserName</code></td>
<td>Specifies the User-Name attribute, which must be sent in the proxy request. If ProxyUserName is not set, the User-Name from the original request packet is used.</td>
</tr>
<tr>
<td><code>%Alias</code></td>
<td>Specifies the value returned from this column that is matched with an existing Steel-Belted Radius Native User entry of the same name. For example, if the value is <code>max1</code>, and a native user called <code>max1</code> exists in the Steel-Belted Radius database, then any return list or checklist attributes, as well as any concurrent connection limit configured for <code>max1</code>, are applied to the user’s connection. If you want to apply concurrent connection limits to users who are being authenticated by means of SQL, you must set up a Native User entry with no password. <strong>NOTE:</strong> Use of <code>%Alias</code> is not recommended. Instead, use <code>%Profile</code>.</td>
</tr>
<tr>
<td><code>%FullName</code></td>
<td>The value returned from this column is interpreted as the full name of the user. This feature is often used to distinguish the user’s full name from the actual User-Name sent in the Access-Request.</td>
</tr>
<tr>
<td>RADIUS attributes</td>
<td>Any RADIUS attribute (preceded by an @) can be returned from the database and mapped into the [Results] section. Use attribute names as they appear in the appropriate .dct files.</td>
</tr>
</tbody>
</table>
where `user_pwd`, `attribs`, `fullname`, and `user_id` are the names of columns in the SQL table, and rasusers is the name of the SQL table itself. The [Results] section of this header file must map the SQL table columns `user_pwd`, `attribs`, and `fullname` to authentication and/or authorization data types; for example.

```
[Results]
Password=1
Profile=2
FullName=3
```

Columns in the SQL query are identified in the [Results] section by number; 1 represents the first column in the SELECT query (from left to right), and if other columns are also referenced, 2 represents the second, and 3 the third.

Along with a number representing the column order, each entry in the [Results] section also specifies the storage format of the column in the SQL table, using the same slash (/), length, and type conventions as the SQL query.

**Default [Results] Parameters**

The DefaultResults flag in the [Settings] section of sqlauth.aut specifies whether default values for `Password`, `Profile`, `Alias`, and `FullName` are automatically bound to the returned SQL data. The default sqlauth.aut file sets it to 0.

With DefaultResults=0, the results list is no longer automatically bound, and only explicit columns in the [Results] section, or embedded Parameters to a stored procedure, are used. This is the recommended setting.

The DefaultResults=1 option remains only for backward-compatibility with old .aut files that rely on the default results behavior to ensure that the set of default columns are automatically bound.

**[Server] Section**

*Used by:* GEE, SPE, SPE+EAP, SPE+MIM  
*Not used by:* EE

Steel-Belted Radius can maintain multiple SQL server connections and authenticate users against authentication databases in a round-robin fashion. This convention distributes the authentication workload across several servers.

The [Server] section of the SQL authentication header file gives Steel-Belted Radius a pool of servers from which to create the round-robin list. The [Server] section names each server that might be used. It also provides rules for when each of the possible servers should be included in (or excluded from) the round-robin list.

```
[Server]
    ServerName=TargetNumber
    ServerName=TargetNumber
    ...
```
Chapter 10: SQL Authentication Files

A Steel-Belted Radius server maintains connectivity with its SQL servers according to the following rules:

- The priority of the server by order. The first entry in the [Server] section has the highest priority.
- By activation target number. The rule for the activation target is that if the number of SQL servers to which Steel-Belted Radius is connected is less than the activation target, Steel-Belted Radius connects to the server and includes it in the round-robin list. While the number of active servers is equal to or greater than the activation target, Steel-Belted Radius does not use that server in the round-robin list. An activation target of 0 indicates that, in the current configuration, this machine is never used.

### [Server/name] Sections

**Used by:** GEE, SPE, SPE+EAP, SPE+MIM  
**Not used by:** EE

You must provide a [Server/name] section for each server you’ve named in the [Server] section, as follows, depending on your operating system:

- **Solaris:***
  
  [Server/name]  
  Connect=username/password@servicename
  
  where the values for username and password are specific to the SQL database, and servicename is the Oracle service name.

- **Windows:***
  
  [Server/name]  
  Connect=DSN=dsnname;UID=username;PWD=password
  
  where the values for dsnname, username, and password are specific to the SQL database you are using.

**NOTE:** Do not use the SA account or leave the password blank.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerName</td>
<td>The name of the header file section that contains configuration information for that server.</td>
</tr>
<tr>
<td>TargetNumber</td>
<td>An activation target number, a number that controls when this server is activated for backup purposes. TargetNumber is optional and may be left blank.</td>
</tr>
</tbody>
</table>
**Last Resort Server**

You may identify a “last resort” SQL server by providing a `LastResort` parameter in one of these `[Server/name]` sections, and setting its value to 1. If a SQL query against some other server results in “no record found,” the authentication server tries the last resort server before accepting or rejecting the user.

In the following example, server `s3` is the last resort server; in the Solaris example, the `@mydb` string refers to the service name for an Oracle database in the `tnsnames.ora` file (the server won’t connect to the Oracle database without this).

- **Solaris:**
  
  ```
  [Server]
  s1=2
  s2=2
  s3=1
  
  [Server/s1]
  Connect=system1/manager
  
  [Server/s2]
  Connect=system2/manager@mydb2
  
  [Server/s3]
  Connect=system3/manager@mydb3
  LastResort = 1
  ```

- **Windows:**
  
  ```
  [Server]
  s1=2
  s2=2
  s3=1
  
  [Server/s1]
  Connect=DSN=dsnname;UID=username;PWD=password
  
  [Server/s2]
  Connect=DSN=dsnname;UID=username;PWD=password
  
  [Server/s3]
  Connect=DSN=dsnname;UID=username;PWD=password
  LastResort = 1
  ```

You might use the `LastResort` parameter to identify your master accounts database. This enables Steel-Belted Radius to authenticate the user in the case where a user account is newly added to the master accounts database but has not yet been propagated to all the SQL databases.

**[Settings] Section**

The `[Settings]` section of the SQL authentication header file defines parameters that control the database connection.

```
[Settings]
Connect=DSN=<dsn_name_here>;UID=<username_for_dB>;PWD=<password_for_dB>
```
SQL=SELECT password, profile FROM userlist WHERE name = %name/40
ParameterMarker=?
MaxConcurrent=1
ConcurrentTimeout=30
ConnectTimeout=25
QueryTimeout=25
WaitReconnect=2
MaxWaitReconnect=360
PasswordFormat = 0
DefaultResults = 0

Table 125: *.aut [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConcurrentTimeout</td>
<td>Specifies the number of seconds a request may wait for execution before it is discarded. Since there may be only up to MaxConcurrent SQL statements executing at one time, new requests must be queued as they arrive until other statements are processed.</td>
</tr>
<tr>
<td>Connect</td>
<td>Specifies the string that must be passed to the database client engine to establish a connection to the database. This string has (or refers to) information about the name of the database, its location on the network, the password required to access it, and so forth. The format of the connect string depends on the type of database you use: Oracle: Connect=&lt;dB_username&gt;/&lt;dB_password&gt; JDBC: Connect=DSN=<a href="">jdbc:provider:driver:dsn_name_here</a>;UID=&lt;username_for_dB&gt;;PWD=&lt;password_for_dB&gt;</td>
</tr>
<tr>
<td>ConnectDelimiter</td>
<td>(JDBC only) Specifies the character used to separate fields (DSN, UID, PWD) in the connect string. Default value is ; (semicolon). If the JDBC connect string requires use of semicolons as part of a field value, you can use this parameter to specify a different delimiter, such as ^ (caret).</td>
</tr>
<tr>
<td>ConnectTimeout</td>
<td>Specifies the number of seconds to wait when attempting to establish the connection to the database before timing out. This value is ignored if the client database engine does not support this feature.</td>
</tr>
</tbody>
</table>
| DefaultResults     | ■ If set to 0, no default values are assumed and the user must explicitly enter all result items (if you are not calling a stored procedure).
■ If set to 1, the default values for Results are used. This is the backward-compatibility setting and the setting if no value is specified in the file. In this case, each Result item must be explicitly specified. |
| Driver             | (JDBC only) Specifies the third-party JDBC driver to load for authentication. For example: Driver=com/provider.jdbc/sqlserver/SQLServerDriver NOTE: Third-party JDBC drivers must be installed in /radius/jre/lib/ext. Refer to the JDBC driver documentation for information on how to install the JDBC driver and supporting files. |
### Table 125: *.aut [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogLevel</td>
<td>Activates logging for the SQL authentication component and sets the rate at which it writes entries to the server log file (.LOG). The LogLevel may be the number 0, 1, or 2, where 0 is the lowest logging level, 1 is intermediate, and 2 is the most verbose. If the LogLevel that you set in the .aut file is different than the LogLevel in radius.ini, the radius.ini setting determines the rate of logging. <strong>GEE/SPE:</strong> The LogLevel is re-read whenever the server receives a HUP signal.</td>
</tr>
<tr>
<td>MaxConcurrent</td>
<td>Specifies the maximum number of instances of a single SQL statement that may be executing at one time.</td>
</tr>
<tr>
<td>MaxWaitReconnect</td>
<td>Specifies the maximum number of seconds to wait after successive failures to reconnect after a failure of the database connection. WaitReconnect specifies the time to wait after failure of the database connection. This value is doubled on each failed attempt to reconnect, up to a maximum of MaxWaitReconnect.</td>
</tr>
<tr>
<td>ParameterMarker</td>
<td>Specifies the character or sequence of characters used as the parameter marker in a parameterized SQL query. Normally, this is the question mark (?), but this could vary among database vendors.</td>
</tr>
</tbody>
</table>
| PasswordFormat    | ■ If set to 0, Steel-Belted Radius tries to determine password format automatically.  
                    ■ If set to 3, Steel-Belted Radius expects the password value encrypted with UNIXcrypt.  
                    By default, the PasswordFormat parameter is not listed in the [Settings] section of the .aut file. |
| QueryTimeout      | Specifies the number of seconds to wait for a response to a query before timing out. This value is passed to the client database engine, which may or may not implement the feature. |
| SQL               | Specifies the SQL statement used to access the password information in the database. The SQL statement may be broken over several lines by ending each line with a backslash. The backslash must be preceded by a space character, and followed by a newline character. The subsequent lines may be indented for better readability. Example:  
                    SQL=SELECT password, profile, fullname  
                    FROM usertable  
                    WHERE username = %name/63s |
| SuccessResult     | Specifies the string that is the expected result of a successful authentication, to be compared to the %result parameter.  
                    If a value is specified for this field, it is used in the following manner upon execution of the SQL statement: if the value of %result is not equal to the value given for this field, the user is rejected. The test for textual equality is not case sensitive.  
                    No such test, or rejection, is performed if no value is specified for this field.  
                    This is a useful technique for coordinating with the custom functionality of stored procedures. |
| UpperCaseName     | Specifies whether the user’s login name should be converted to uppercase characters before using it in the SQL statement execution.  
                    ■ 0 – Use the name exactly as received.  
                    ■ 1 – Convert the name to uppercase. |
The [Strip] sections of the SQL authentication header file allow User-Name stripping to occur. These sections enable Steel-Belted Radius to identify the username that the SQL database expects by stripping the incoming User-Name attribute value of realm names and other “decorations.”

You may or may not need to employ User-Name stripping for SQL authentication. Your need for this feature depends upon the naming conventions that you employ on your network and in your SQL database entries. Steel-Belted Radius’s usual name parsing features work independently of this feature.

The following [Strip] syntax is available to enable and configure User-Name stripping for SQL authentication:

```
[Strip]
Authentication=Yes

[StripPrefix]
String
String
:

[StripSuffix]
String
String
:
```

<table>
<thead>
<tr>
<th>Table 126: *.aut [Strip] Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Table 126: *.aut [Strip] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>[StripPrefix]</td>
<td>Lists strings that are to be stripped from the beginning of the User-Name value. The strings are listed in order of priority. A string that appears earlier in the list takes precedence over later strings. In the following example, if the incoming User-Name is “seattleUser201”, the stripped name is “User201”. If the incoming User-Name is “seatac2000”, the stripped name is “tac2000”.</td>
</tr>
<tr>
<td>String</td>
<td>Each String that you provide in a [Strip] section may be a character string, or a regular expression according to the following rules: ? is a wildcard character. A dash (-) indicates a range of alphanumeric characters; brackets must enclose lists of characters or ranges. For example, [A-Za-z] means any letter and [0-9.] means any number, including decimal points and commas. A backslash () followed by a non-alphanumeric character indicates that character literally, for example \ indicates the question mark. \ is also used as an escape character, as follows:</td>
</tr>
<tr>
<td></td>
<td>\a          bell (7)</td>
</tr>
<tr>
<td></td>
<td>\b          backspace (8)</td>
</tr>
<tr>
<td></td>
<td>\t          tab (9)</td>
</tr>
<tr>
<td></td>
<td>\n          newline (10)</td>
</tr>
<tr>
<td></td>
<td>\v          vertical tab (11)</td>
</tr>
<tr>
<td></td>
<td>\f          formfeed (12)</td>
</tr>
<tr>
<td></td>
<td>\r          return (13)</td>
</tr>
<tr>
<td></td>
<td>\nn        hex value, where nn are 2 hex digits</td>
</tr>
<tr>
<td></td>
<td>\nnn       decimal value, where nnn are 3 decimal digits</td>
</tr>
<tr>
<td>[StripSuffix]</td>
<td>Lists strings that are to be stripped from the end of the User-Name value. Conventions are the same as for [StripPrefix].</td>
</tr>
</tbody>
</table>
Chapter 11

SQL Accounting Files

This chapter describes the files used for SQL accounting in Steel-Belted Radius.
SQL Accounting Header (.acc) File

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM, EE  
**Not Used By:** —

The header file used to configure SQL accounting methods must have a `.acc` extension: for example, `sqlacct.acc`. The format of a header file is comparable to that of a Windows INI file: it is composed of several sections; section names are enclosed in brackets; each section may contain multiple parameter/value pairs.

### [Bootstrap] Section

The [Bootstrap] section of the SQL accounting header file (Table 127) specifies information used to load and start the SQL accounting module.

```plaintext
[Bootstrap]
LibraryName=sqlacct.dll
Enable=0
InitializationString=
```

**Table 127: *.acc [Bootstrap] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibraryName</td>
<td>Specifies the name of the SQL accounting module.</td>
</tr>
<tr>
<td>Solaris: Enter <code>radsql_acct_ora.so</code> (for Oracle) or <code>radsql_acct_jdbc.so</code> (for JDBC).</td>
<td></td>
</tr>
<tr>
<td>Windows: Enter <code>sqlacct.dll</code>.</td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td>Specifies whether the SQL accounting method is enabled.</td>
</tr>
<tr>
<td>&quot;If set to 0, SQL accounting is disabled.</td>
<td></td>
</tr>
<tr>
<td>&quot;If set to 1, SQL accounting is enabled.</td>
<td></td>
</tr>
<tr>
<td>Default value is 0.</td>
<td></td>
</tr>
<tr>
<td>InitializationString</td>
<td>Not used.</td>
</tr>
</tbody>
</table>

### [Settings] Section

The [Settings] section of the SQL accounting header file defines parameters that control the database connection.

**Table 128: *.acc [Settings] Syntax**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| ConcurrentTimeout  | Specifies the number of seconds a request may wait for execution before it is discarded. Since there may be up to MaxConcurrent SQL statements executing at one time, as new requests arise they must be queued, waiting for other statements to complete.  
ConcurrentTimeout may be overridden for any particular statement in the [Type/statement] section for that statement. |
### Connect
Specifies the string that must be passed to the database client engine to establish a connection to the database. This string has (or refers to) information about the name of the database, its location on the network, the password required to access it, and so forth.

The format of the connect string depends on the type of database you use:

- **Oracle:**
  ```
  Connect=<dB_username>/<dB_password>
  ```

- **JDBC:**
  ```
  Connect=DSN=<jdbc:provider:driver:dsn_name_here>;UID=<username_for_dB>;PWD=<password_for_dB>
  ```

### ConnectDelimiter (JDBC only)
Specifies the character used to separate fields (DSN, UID, PWD) in the connect string.

Default is ; (semicolon). If the JDBC connect string requires use of semicolons as part of a field value, you can use this parameter to specify a different delimiter, such as ^ (caret).

### ConnectTimeout
Specifies the number of seconds to wait when attempting to establish the connection to the database before timing out. This value is passed to the client database engine, which may or may not implement the feature.

### Driver (JDBC only)
Specifies the third-party JDBC driver to load for accounting.

For example:

- **Driver**=
  ```
  com/provider/jdbc/sqlserver/SQLServerDriver
  ```

**NOTE:** Third-party JDBC drivers must be installed in `/radius/jre/lib/ext`. Refer to the JDBC driver documentation for information on how to install the JDBC driver and supporting files.

### LogLevel
Activates logging for the SQL accounting component and sets the rate at which it writes entries to the server log file (.LOG). The LogLevel may be the number 0, 1, or 2, where 0 is the lowest logging level, 1 is intermediate, and 2 is the most verbose. If the LogLevel that you set in the *.acc file is different than the LogLevel in `radius.ini`, the `radius.ini` setting determines the rate of logging.

Default value is 2.

**GEE/SPE:** The LogLevel is re-read whenever the server receives a HUP signal.

### MaxConcurrent
Specifies the maximum number of instances of a single SQL statement that may be executing at one time.

`MaxConcurrent` may be overridden for any particular statement in the [Type/statement] section for that statement.

### MaxWaitReconnect
Specifies the maximum number of seconds to wait after successive failures to reconnect after a failure of the database connection.

WaitReconnect specifies the time to wait after failure of the database connection. This value is doubled on each failed attempt to reconnect, up to a maximum of MaxWaitReconnect.

### ParameterMarker
Specifies the character or sequence of characters used as the parameter marker in a parameterized SQL query.

Default is ? (question mark).

---

### Table 128: *.acc [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Connect            | Specifies the string that must be passed to the database client engine to establish a connection to the database. This string has (or refers to) information about the name of the database, its location on the network, the password required to access it, and so forth. The format of the connect string depends on the type of database you use:  
Oracle:  
```
Connect=<dB_username>/<dB_password>
```  
JDBC:  
```
Connect=DSN=<jdbc:provider:driver:dsn_name_here>;UID=<username_for_dB>;PWD=<password_for_dB>
```  
| ConnectDelimiter   | Specifies the character used to separate fields (DSN, UID, PWD) in the connect string.  
Default is ; (semicolon). If the JDBC connect string requires use of semicolons as part of a field value, you can use this parameter to specify a different delimiter, such as ^ (caret). |
| ConnectTimeout     | Specifies the number of seconds to wait when attempting to establish the connection to the database before timing out. This value is passed to the client database engine, which may or may not implement the feature. |
| Driver             | Specifies the third-party JDBC driver to load for accounting.  
For example:  
```
Driver=com/provider/jdbc/sqlserver/SQLServerDriver
```  
**NOTE:** Third-party JDBC drivers must be installed in `/radius/jre/lib/ext`. Refer to the JDBC driver documentation for information on how to install the JDBC driver and supporting files. |
| LogLevel           | Activates logging for the SQL accounting component and sets the rate at which it writes entries to the server log file (.LOG). The LogLevel may be the number 0, 1, or 2, where 0 is the lowest logging level, 1 is intermediate, and 2 is the most verbose. If the LogLevel that you set in the *.acc file is different than the LogLevel in `radius.ini`, the `radius.ini` setting determines the rate of logging.  
Default value is 2.  
**GEE/SPE:** The LogLevel is re-read whenever the server receives a HUP signal. |
| MaxConcurrent      | Specifies the maximum number of instances of a single SQL statement that may be executing at one time.  
MaxConcurrent may be overridden for any particular statement in the [Type/statement] section for that statement. |
| MaxWaitReconnect   | Specifies the maximum number of seconds to wait after successive failures to reconnect after a failure of the database connection.  
WaitReconnect specifies the time to wait after failure of the database connection. This value is doubled on each failed attempt to reconnect, up to a maximum of MaxWaitReconnect. |
| ParameterMarker    | Specifies the character or sequence of characters used as the parameter marker in a parameterized SQL query.  
Default is ? (question mark). |
[Type] Sections

Each entry in the [Type] section of the SQL accounting header file maps an Acct-Status-Type attribute value to a statement name that you may assign arbitrarily. The statement name is then used to look up another section in the header file that describes that statement. The secondary section names are composed as [Type/statement], where statement is the arbitrarily assigned name for the statement.

For example, to perform separate accounting updates for network access device and user activity, you might provide the following [Type] and [Type/statement] sections:

```
[Type]
1=user
2=user
3=user
7=nas
8=nas
639=nas
28=nas

[Type/user]
SQL=INSERT INTO usagelog \
  (Time, NASAddress, SessionID, \n  Type, Name, BytesIn, BytesOut) \
VALUES \n  (%TransactionTime/t, %NASAddress, \n  @Acct-Session-Id, @Acct-Status-Type, \n  %FullName/40s, @Acct-Input-Octets, \n  @Acct-Output-Octets)

[Type/nas]
SQL=INSERT INTO  ...
```

Note the numeric values used in the [Type] section above. The Acct-Status-Type values 1, 2, 3, 7, and 8 have been reserved by the RADIUS accounting standard with names and meanings, as described in Table 129.
Additional values for `Acct-Status-Type` have been defined by network access device vendors for use with their equipment. These vendor-specific values may also be listed in the `[Type]` section.

**[Type/statement] Sections**

Table 130 lists the parameters that may be present in a `[Type/statement]` section of the SQL accounting header file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL</td>
<td>Specifies the exact SQL statement used to update the SQL database with accounting information. The SQL statement may be broken over several lines by ending each line with a backslash. The backslash must be preceded by a space character, and followed by a newline. The subsequent lines may be indented for better readability. For example:</td>
</tr>
<tr>
<td></td>
<td><code>SQL=INSERT INTO accounting\(TransTime, FullName, Authenticator, NASName, NASAddress, Type, PacketsIn, PacketsOut) VALUES (%TransactionTime/t, %FullName/40s, %AuthType/40s, %NASName/40s, %NASAddress, %Type, @Acct-Input-Packets/n, @Acct-Output-Packets/n)</code></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You should include the /t (timestamp) data type qualifier with the <code>%TransactionTime</code> argument in SQL statements. If you do not, the <code>%TransactionTime</code> output is formatted as character, with differing results on JDBC and Oracle.</td>
</tr>
<tr>
<td>MaxConcurrent</td>
<td>If present, <code>MaxConcurrent</code> overrides the value of <code>MaxConcurrent</code> specified in the <code>[Settings]</code> section for this particular statement.</td>
</tr>
<tr>
<td>ConcurrentTimeout</td>
<td>If present, <code>ConcurrentTimeout</code> overrides the value of <code>ConcurrentTimeout</code> specified in the <code>[Settings]</code> section for this particular statement.</td>
</tr>
<tr>
<td>QueryTimeout</td>
<td>If present, <code>QueryTimeout</code> overrides the value of <code>QueryTimeout</code> specified in the <code>[Settings]</code> section for this particular statement.</td>
</tr>
</tbody>
</table>
[TypeNames] Section

Each entry in the [TypeNames] section of the SQL accounting header file maps an Acct-Status-Type attribute value to a string. If a %Type parameter is present in the corresponding SQL statement, this %Type parameter contains the given string.

If no string is given for a particular Acct-Status-Type, when an accounting request of that type is received, %Type is set to the numeric value of the Acct-Status-Type attribute, formatted as a string.

The syntax for the [TypeNames] section is as follows:

\[
\begin{align*}
\text{[TypeNames]} \\
\text{TypeID} &= \text{TypeName} \\
\text{TypeID} &= \text{TypeName} \\
& \cdots
\end{align*}
\]

You can include RADIUS standard and vendor-specific accounting packet types; for example:

\[
\begin{align*}
\text{[TypeNames]} \\
1 &= \text{Start} \\
2 &= \text{Stop} \\
3 &= \text{Interim} \\
7 &= \text{On} \\
8 &= \text{Off} \\
639 &= \text{AscendType} \\
28 &= \text{3ComType}
\end{align*}
\]

Working With Stored Procedures

A stored procedure is a sequence of SQL statements that form a logical unit and perform a particular task. You can use stored procedures to encapsulate a set of queries or operations that can be executed repeatedly on a database server. For example, you can code operations on an employee database, such as password lookup, as stored procedures that can be executed by application code. For more information on stored procedures, see the Steel-Belted Radius Administration Guide.

The SQL example in the previous section could be replaced by a custom stored procedure. This stored procedure might look something like the following:

```
PROCEDURE myProc
(
    ttime in     varchar2,
    nasaddr in   varchar2,
    sessid in    varchar2,
    ttype in     varchar2,
    uname in     varchar2,
    bytein in    varchar2,
    byteout in   varchar2
);
END myProc;
```

CREATE OR REPLACE PACKAGE BODY myPack1 IS
PROCEDURE myProc
(
[...]
);
ttime in varchar2,
nasaddr in varchar2,
sessid in varchar2,
ttype in varchar2,
uname in varchar2,
bytein in varchar2,
byteout in varchar2
)
IS
BEGIN
INSERT INTO usagelog
( Time, NASAddress, SessionID, Type, Name,
  BytesIn, BytesOut )
VALUES
( ttime, nasaddr, sessid, ttype, uname, bytein,
  byteout );
END myProc;
END myPack1;

When you invoke the stored procedure, delineate each parameter as an input (!i), output (!o), or input/output (!io) variable.

This stored procedure can be invoked with the following connect string in the radsql.acc file:

```
SQL=BEGIN myPack1.myProc(%TransactionTime!i,
  %NASAddress!i, @Acct-Session-Id!i, %Type!i,
  %FullName!i, @Acct-Input-Packets!i,
  @Acct-Output-Packets!i); END;
```

**Load Balancing Example (GEE/SPE only)**

The following excerpt from a .acc example file configures load balancing between two SQL servers (so that the work load is shared nearly equally between two servers). The tradeoff with this technique is that the data is split between two servers and must be reintegrated when processed. For example, the Accounting-START for an end-user may be stored on one server and the corresponding Accounting-STOP on the other.

```
[Server]
s1=2
s2=2

[Server/s1]
Connect=system/*********@thor

[Server/s2]
Connect=system/*********@odin

[Type]
1=User
2=User
3=User

[Type/User]
SQL=INSERT INTO acct1(TransTime, FullName, 
  Authenticator, NASName, NASAddress, Type, 

PacketsIn, PacketsOut) \nVALUES (%TransactionTime/t, %FullName/40s, \
%AuthType/40s, %NASName/40s, %NASAddress, \
%Type, @Acct-Input-Packets/n, \n@Acct-Output-Packets/n)
Chapter 12
LDAP Authentication Files

This chapter describes the files used to configure LDAP authentication in Steel-Belted Radius.
LDAP Authentication Header (.aut) File

**Used by:** GEE, SPE, SPE + EAP, SPE + MIM, EE*

**Not Used By:** —

The LDAP authentication header file is located in the same directory that contains the Steel-Belted Radius service (normally `C:\Program Files\Juniper Networks\Steel-Belted Radius\Service`) or daemon. The header file must have the extension `.aut` and is usually called `ldapauth.aut`.

The structure of the LDAP authentication header file is comparable to that of a Windows INI file. An LDAP authentication header file consists of several sections, where each section may contain multiple entries. Section names are enclosed in square brackets, for example `[Bootstrap]`. Each entry in the section appears on one line, and is of the form `parameter = value`. A section ends at the next section, or at the end of the file. Everything to the right of a semicolon (`;`) is ignored until the end of that line.

**LDAP Authentication Variable Names**

When Steel-Belted Radius extracts RADIUS attribute values from the incoming Access-Request and adds them to the Variable Table, the name that it gives to each variable is the same as the name of the corresponding attribute, for example User-Name or Calling-Station-ID. You may refer to the variable by this name in any subsequent entry in the .aut header file. This convention means that RADIUS attribute names are treated as reserved keywords. However, the .aut header file syntax also permits you to assign the value of an incoming RADIUS attribute to any variable.

When the LDAP Search request returns LDAP attribute values, they are added to the Variable Table. Steel-Belted Radius gives each variable the name of the corresponding LDAP attribute. In the schema illustrated above, this would produce variable names such as User-Secret and Last-Name. For the names to use in your own .aut header file, consult your LDAP database schema. Like RADIUS attribute names, LDAP attribute names are treated as reserved keywords. However, the .aut header file syntax permits you to assign the value of a returned LDAP attribute to any variable.

**[Bootstrap] Section**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE

**Not used by:** —

The [Bootstrap] section of the LDAP authentication header file specifies information that Steel-Belted Radius uses to load and start the LDAP Authentication plug-in.

After you edit `ldapauth.aut` and restart Steel-Belted Radius, the InitializationString value that you entered in the [Bootstrap] section of `ldapauth.aut` appears in the Authentication Methods list in the Authentication Policies panel. You can then enable, disable, or prioritize this method like any other entry in the list.
You can configure more than one LDAP authentication method. Each requires its own .aut file in the same directory as ldapauth.aut. The [Bootstrap] section of each .aut file must provide a LibraryName of ldapauth.so (for Solaris/Linux) or ldapauth.dll (for Windows). The InitializationString in each .aut file must be unique, so that you can distinguish between authentication methods in the Authentication Policies panel.

### Table 131: *.aut [Bootstrap] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LibraryName</td>
<td>Specifies the name of the LDAP authentication module. Value must be ldapauth.so for Solaris/Linux and ldapauth.dll for Windows.</td>
</tr>
<tr>
<td>Enable</td>
<td>■ If set to 1, the LDAP authentication module is enabled.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, the LDAP authentication module is disabled, and the authentication method is unavailable and does not appear in the Authentication Methods list in the Authentication Policies panel. Default value is 0.</td>
</tr>
<tr>
<td>InitializationString</td>
<td>Specifies the identifier for the authentication method, which appears in the Authentication Methods list in the Authentication Policies panel. The name of each authentication method must be unique. If you create additional .aut files to implement authentication against multiple databases, be sure that each .aut file has a unique InitializationString value. Default value is LDAP.</td>
</tr>
</tbody>
</table>

**[Attributes/name] Sections**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE
**Not used by:** —

LDAP database entries may have many attributes, many of which may be irrelevant to the authentication process. An LDAP Search returns all of the attributes associated with an LDAP entry. Therefore, when specifying an LDAP Search for authentication purposes, you may want to provide a list of specific LDAP attributes relevant to Steel-Belted Radius. Only these attributes are placed in the Variable Table.

Each [Attributes/name] section in the LDAP authentication header file lists LDAP attributes relevant to a specific LDAP Search request. The syntax is as follows:

```
[Attributes/name]
attribute
attribute
;
```

where attribute is the name of an LDAP attribute and name is an arbitrary name for the section. You must type the attribute names exactly as they appear in your LDAP database schema. Use one line per attribute. For example:

```
[Attributes/InterestingAttributes]
User-Secret
RADIUS-Profile
Inactivity-Timeout
```
An [Attributes/name] section is associated with a Search request by referencing it from within a [Search/name] section using the Attributes parameter. For example:

```
[Search/DoLdapSearch]
Attributes = InterestingAttributes
```

If the Attributes parameter is omitted from a [Search/name] section, Steel-Belted Radius retains all of the attributes associated with the LDAP entry. Of these attributes, Steel-Belted Radius uses only those referenced in the .aut header file; all others stay in the Variable Table until the authentication transaction is complete and the table is discarded.

For BindName authentication, you must ensure that the [Attributes/name] section lists the attribute in which the user’s password is stored and that your [Response] section assigns the value of this attribute to the outgoing %Password parameter. Steel-Belted Radius completes authentication by comparing the returned %Password value with the password that arrived in the Access-Request. For example:

```
[Attributes/InterestingAttributes]
User-Secret
RADIUS-Profile
Inactivity-Timeout

[Response]
%Password = User-Secret
%Profile = RADIUS-Profile
Vendor-Specific-NAS-Attribute = Inactivity-Timeout
```

**[Response] Section**

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE*

Not used by: —

During an authentication transaction, the [Response] section is the last section in the LDAP authentication header file to be processed. At this point in processing, all Bind and Search requests to the LDAP database have been completed.

The [Response] section tells Steel-Belted Radius what to do with the information that it has retrieved from the incoming Access-Request and from the LDAP database. The goal at this point is for Steel-Belted Radius to complete authentication and issue an Access-Response to the RADIUS client.

The [Response] section syntax is as follows:

```
[Response]
attribute = variable
attribute = variable
```

where attribute is the name of a RADIUS attribute or other special item needed to complete authentication, and variable is the name of a variable in the Variable Table. The end result of the [Response] syntax is that the value in the variable is assigned to the attribute.
An IP pool can be returned for any attribute of the appropriate type. If the returned string appears to be an IP address (that is, in the format, a.b.c.d), it is considered an IP address; otherwise, it is considered a address pool, from which an IP address is allocated.

attribute may be the name of a RADIUS attribute, or it may be one of the following keywords, which identify various special items associated with Steel-Belted Radius. Each of these keywords begins with the percent sign (%) to distinguish it clearly from the RADIUS attributes.

Table 132: *.aut [Response] Syntax

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>%LoginLimit</td>
<td>The name of the variable specifying the Maximum Concurrent Connection limits.</td>
</tr>
<tr>
<td>(GEE/SPE only)</td>
<td></td>
</tr>
</tbody>
</table>
| %Password       | For BindName authentication, you must provide a %Password entry in the [Response] section and you must assign it the value of the password attribute retrieved from the LDAP database. Steel-Belted Radius validates the password received in the Access-Request by comparing it with the value assigned to %Password. If the passwords don’t match, the request is rejected.  

**NOTE:** The user’s password may be in clear text, or encrypted with UNIXcrypt or a SHA1 + Base64 hash.  
For Bind authentication, omit %Password. Once processing reaches the [Response] section, the password has already been validated. |
| %Profile        | The name of a Profile entry in the Steel-Belted Radius database.  
If the password has been validated (by BindName or Bind), with %Profile listed in the [Response] section, %Profile may be set to any variable, for example:  

%Profile = userpolicy  
When the search filter is set to find a user or object in the LDAP database that includes the userpolicy LDAP attribute, this value is retrieved and returned to the Steel-Belted Radius database so that it may be matched with an existing Profile entry of the same name. If the userpolicy LDAP attribute is multi-valued, the first value of userpolicy is used and subsequent values are ignored.  
If the value of userpolicy is “prof1” and a Profile called prof1 exists in the Steel-Belted Radius database, any return list or checklist attributes in prof1 are applied to the user’s connection.  
If the value returned from LDAP cannot be matched with an existing Profile in the Steel-Belted Radius database, the user is rejected due to “Insufficient Resources.” |
| %ProxyRealm     | The realm to which the authentication must be proxied. If ProxyRealm is not set, Routed Proxy does not occur. |
| (GEE/SPE only)  |                                                                          |
| %ProxyUserName  | The User-Name attribute, which must be sent in the proxy request. If ProxyUserName is not set, the User-Name from the original request packet is used. |
| (GEE/SPE only)  |                                                                          |
Table 132: *.aut [Response] Syntax (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>%Alias</td>
<td>The name of a Native User entry in the Steel-Belted Radius database. If the password has been validated (by BindName or Bind), with %Alias listed in the [Response] section, %Alias may be set to any variable, for example: %Alias = userpolicy.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>: You are strongly recommended to use %Profile, as use of %Alias has been deprecated.</td>
</tr>
<tr>
<td></td>
<td><strong>GEE/SPE</strong>: The %LoginLimit value lets you implement the concurrent connection limits previously available through %Alias.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: Native User entries without passwords automatically cannot be authenticated. This is a safety feature built into Steel-Belted Radius. Therefore, setting up Native User entries in preparation for using the Alias parameter with LDAP authentication does not pose a “back door” security risk.</td>
</tr>
<tr>
<td></td>
<td>Generally, even if a very large number of users reside in the LDAP database, you need to add only one or two Native User entries to the Steel-Belted Radius database. The concurrent connection limit associated with a single Native User entry may be applied to any number of users in the LDAP database. Often a Native User entry with a connection limit of 1, and a second Native User entry with a connection limit of 2, is sufficient for the entire LDAP database.</td>
</tr>
<tr>
<td></td>
<td>For example, analog users may be allowed a connection limit of 1, while ISDN users are allowed a connection limit of 2.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The Native User authentication method displayed in the Authentication Policies panel does not need to be activated for the Alias feature to work.</td>
</tr>
<tr>
<td>%FullName</td>
<td>The fully distinguished name of the User, for Steel-Belted Radius accounting purposes. This is the exact name against which authentication was performed. Depending on what may have occurred during Steel-Belted Radius name parsing, this name may or may not be different from the value of the User-Name attribute as it originally arrived in the Access-Request.</td>
</tr>
</tbody>
</table>

[Search/\texttt{name}] Sections

**Used by**: GEE, SPE, SPE + MIM, SPE + EAP, EE*

**Not used by**: —

Each [Search/\texttt{name}] section in the LDAP authentication header file specifies the complete details of one LDAP Search request. You can use the same Search request on various databases, because the details of the database connection are specified separately.

For BindName authentication, you must ensure that each [Search/\texttt{name}] section searches for a database entry that matches the incoming username and retrieves from it an attribute containing that user’s password. Steel-Belted Radius must compare this password to the one it received in the incoming Access-Request packet.

A [Search/\texttt{name}] section may retrieve other LDAP attributes as well; however, if you are authenticating with BindName, the user’s password is a minimum requirement. Use the Attributes parameter to specify the list of items you want returned.
For example:

```
[Search/DoLDAPSearch]
Base = ou=Special Users, o=bigco.com
Scope = 1
Filter = uid=<User-Name>
Attributes = InterestingAttributes
Timeout = 20
%DN = dn

[Attributes/InterestingAttributes]
User-Secret
RADIUS-Profile
Inactivity-Timeout

[Response]
%Password = User-Secret
%Profile = RADIUS-Profile
Vendor-Specific-NAS-Attribute = Inactivity-Timeout
```

### Table 133: *.aut [Search/name] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>%DN</td>
<td>Specifies a variable into which the distinguished name that results from the Search should be placed.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Specifies the LDAP attributes relevant to Steel-Belted Radius, by referencing an [Attributes/name] section elsewhere in the same .aut file.</td>
</tr>
<tr>
<td>Base</td>
<td>Specifies the distinguished name (DN) of the entry that serves as the starting point for the search. This filter is a template for an LDAP distinguished name string. The filter follows conventional LDAP syntax and may be as simple or as complex as LDAP syntax permits. It may also include replacement variables from the Variable Table. Each replacement variable consists of the variable name enclosed in angle brackets ( &lt;&gt; ). Upon execution of the LDAP Search request, the value of the variable replaces the variable name.</td>
</tr>
<tr>
<td>OnFound (GEE/SPE only)</td>
<td>Specifies the next request section when data is found. The value of this parameter is a string, name. The name specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same .aut file. If there is no next request section, the overall operation succeeds. This can be overridden using the $reject keyword, which causes the operation to fail when data is found.</td>
</tr>
<tr>
<td>OnNotFound (GEE/SPE only)</td>
<td>Specifies the next request section when data is not found. The value of this parameter is a string, name. The name specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same .aut file. If there is no next request section, the overall operation fails. This can be overridden using the $accept keyword, which causes the operation to succeed when data is not found.</td>
</tr>
<tr>
<td>Search (Optional)</td>
<td>Specifies specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same .aut file. Steel-Belted Radius tries this Search request next, if the current Search yields no result. Note that each [Search/name] section may contain at most one Search parameter.</td>
</tr>
</tbody>
</table>
The Search parameter can be used in one [Search/name] section after another to create a serial “chain” of Search requests. Every Search in the chain is tried. If any Search fails to return data, the Access-Request is rejected.

An example of a two-part chained Search follows:

```
[Settings]
Search = DoLdapSearch

[Search/DoLdapSearch]
Base = ...
Filter = ...
Search = GetMoreLdapInfo

[Search/GetMoreLdapInfo]
Base = ...
Scope = ...
Filter = ...
```

Search sequencing is flexible. GEE/SPE users can proceed to a new search even if the current search returns no data by using the $reject parameter. All editions can override search results using the $reject and $accept keywords. The following is an example of flexible searching:

```
[Search/DoSearch2]
Base = o=xyz.com
Scope = 2
Filter = uid=<User-Name>
Attributes = AttrList
Timeout = 20
%DN = dn
OnFound = DoSearch8
OnNotFound = DoSearch9

[Search/DoSearch8]
Base = o=xyz.com
Scope = 2
Filter = uid=<User-Name>
```

Table 133: *.aut [Search/name] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Specifies the filter to apply to the search. This filter is a template for an LDAP Search string. The filter follows conventional LDAP syntax and may be as simple or as complex as LDAP syntax permits, with multiple attribute/value assertions in boolean combination. It may also include replacement variables from the Variable Table. Each replacement variable consists of the variable name enclosed in angle brackets ( &lt; &gt; ). Upon execution of the LDAP Search request, the value of the variable replaces the variable name. For example, a Search template that uses the User-Name and Service-Type attributes from the RADIUS request might look like this: <code>(&amp; (uid = &lt;User-Name&gt;) (type = &lt;Service-Type&gt;))</code></td>
</tr>
<tr>
<td>Scope</td>
<td>Specifies the scope of the search; 0 (search the base), 1 (search all entries one level beneath the base), or 2 (search the base and all entries beneath the base at any level).</td>
</tr>
</tbody>
</table>
Attributes = AttrList
Timeout = 20
%DN = dn
OnNotFound = DoSearch9

[Search/DoSearch9]
Base = o=xyz.com
Scope = 2
Filter = uid=<User-Name>
Attributes = AttrList
Timeout = 20
%DN = dn
OnNotFound = $accept

[Request] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE*
Not used by: —

The [Request] section of the LDAP authentication header file indicates which RADIUS attribute values Steel-Belted Radius extracts from the incoming Access-Request. Steel-Belted Radius places these values in the Variable Table before moving on to the LDAP Bind and Search requests indicated in the file.

The syntax is as follows:

```
[Request]
attribute = variable
attribute = variable
```

where `attribute` is the name of a RADIUS attribute or other special item associated with the incoming Access-Request, and `variable` is the name of a variable in the Variable Table. The end result of the [Request] syntax is that the value in the incoming attribute is assigned to this variable.

`attribute` may be the name of a RADIUS attribute, or it may be one of the following keywords, which identify various special items also associated with the connection request. Note that each of these keywords begins with the percent sign (%) to strongly distinguish it from the RADIUS attributes.

Table 134: *.aut [Request] Syntax

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>%OriginalUserName</td>
<td>The original full identification of the user, prior to any processing (that is, user@realm).</td>
</tr>
<tr>
<td>%User</td>
<td>The user portion of OriginalUserName (the section before @).</td>
</tr>
<tr>
<td>%UserName</td>
<td>The full user identification (user and realm strings) after all stripping and processing has been performed.</td>
</tr>
<tr>
<td>%Name</td>
<td>Synonym for UserName.</td>
</tr>
</tbody>
</table>
variable may be omitted from any [Request] entry. If so, the value in the incoming attribute is assigned to a variable named attribute.

[Request]
attribute =

In the following [Request] section example, the nasid variable receives the value of the NAS-Identifier attribute from the request packet, the Service-Type variable receives the value of the Service-Type attribute, and the %NASAddress variable receives the NAS address in dotted notation.

[Request]
NAS-Identifier = nasid
Service-Type =
%NASAddress =

[Defaults] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE
Not used by: —

The [Defaults] section of the LDAP authentication header file lets you add entries to the variable table before the request is processed. You can reference these variables in your query, even if they are not supplied in the request. Any variable not listed in the [Defaults] section is initialized to a null value.
The format of each [Defaults] entry is:

```
variable = value
```

where `variable` is the name of a variable and `value` is the value you want to assign to it. For example:

```
[Defaults]
Default-User=SSStudent

[Search/Radius]
Base = ou=people,dc=funk,dc=com
Filter = uid=<Default-User>
Scope = 2
Attributes = RadiusAttrs
Timeout = 20
%DN = dn
```

In this example, the `Default-User` variable is not created during request processing by the LDAP plugin. Instead, the `Default-User` variable is inserted into the variable table by the entry in the [Defaults] section, and then substituted into the Filter setting in the [Search/Radius] section.

You can use the [Defaults] section to specify values for any variable, including temporary variables and those that represent RADIUS attributes or LDAP attributes. This way, if the Access-Request packet and LDAP database do not provide Steel-Belted Radius with all of the values that it needs to respond to an Access-Request, in each case it has an acceptable alternative value that can be used instead.

You can store multiple values for any variable; if that variable is mapped to a RADIUS attribute, all values are returned in the RADIUS response. Multiple entries set within this section are considered multiple values of the same variable.

Variable values are not additive between this section and each search. Therefore, if a search returns one or more values, all current values are replaced.

---

**NOTE:** The [Defaults] section is the only section in the header file that lets you assign static values to variables.

---

**[Server/name] Sections**

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE

**Not used by:** —

Several sections of the LDAP authentication header file work together to configure the connection between the Steel-Belted Radius server and the LDAP database server(s) that are being used to provide external database authentication. The sections are [Server], [Server/name], and [Settings].

Each [Server/name] section of the LDAP authentication header file contains configuration information about a single LDAP server. You must provide a [Server/name] section for each server you’ve named in the [Server] section. For example:
[Server]
s1=
s2=

[Server/s1]
Host = ldap_1
Port = 389

[Server/s2]
Host = 130.4.67.1
LastResort = 1

Table 135 lists the settings that may be present in a [Server/name] section:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind</td>
<td>For Bind authentication, you must specify a Bind template in the [Settings] section of the LDAP authentication header file. The Bind template must follow conventional LDAP syntax. It may be as simple or as complex as LDAP syntax permits, with multiple attribute/value assertions in boolean combination. It may also include replacement variables from the Variable Table. Each replacement variable consists of the variable name enclosed in angle brackets (&lt;&gt;). Upon execution of the LDAP Bind request, the value of the variable replaces the variable name. For example, a Bind template that uses the User-Name attribute from the RADIUS request might look like this: <code>uid=&lt;User-Name&gt;, ou=Special Users, o=bigco.com</code></td>
</tr>
<tr>
<td>BindName</td>
<td>For BindName authentication, the BindName parameter specifies the distinguished name (DN) to be used in the Bind request that connects to the LDAP server. The [Server/name] section lets you specify a unique BindName for a specific server. Use the [Settings] section to specify a default BindName to use for all servers. For Bind authentication, omit all Bind, BindName and BindPassword parameters and use the Bind parameter in the [Settings] section. See “[Settings] Section” on page 265.</td>
</tr>
<tr>
<td>BindPassword</td>
<td>For BindName authentication, you must provide a BindPassword. The BindPassword specifies the password to be used in the Bind request that connects to the LDAP server. The [Server/name] section lets you specify a unique BindPassword for a specific server. Use the [Settings] section to specify a default BindPassword to use for all servers. For Bind authentication, omit the BindName and BindPassword parameters. Use the Bind parameter instead.</td>
</tr>
<tr>
<td>Certificates</td>
<td>Specifies the path of the certificate database for use with SSL. This path must not end in a filename. The certificate database must be the <code>cert7.db</code> and <code>key3.db</code> files used by Netscape Communicator 4.x or later.</td>
</tr>
<tr>
<td>ConnectTimeout</td>
<td>Specifies the number of seconds to wait when attempting to establish the connection to the database before timing out. This value is passed to the client database engine, which may or may not implement the feature.</td>
</tr>
</tbody>
</table>
### FlashReconnect
If the server is down when performing a Bind or a Search, setting this parameter to 1 triggers a reconnection attempt before rejecting the request. Therefore, requests are not rejected due to inactivity timeouts. This setting applies to a particular server. To apply it for all servers, place it in the [Settings] section.

### Host
The host name or IP address of the LDAP server.

### LastResort
You may identify a “last resort” LDAP server by providing a LastResort parameter in one of these [Server/name] sections, and setting its value to 1. If an LDAP query against some other server results in “no record found,” the authentication server tries the last resort server before accepting or rejecting the user. You might use the LastResort parameter to identify your master accounts database. This enables Steel-Belted Radius to cover the case in which a user account is newly added but has not yet been propagated to all the LDAP databases.

### LdapVersion
Specifies the version of LDAP protocol, if needed to override the default given in the [Settings] section.

### MaxConcurrent
Specifies the maximum number of instances of a single LDAP request that may be executing at one time.

### MaxWaitReconnect
Specifies the maximum number of seconds to wait after successive failures to reconnect after a failure of the database connection. WaitReconnect specifies the time to wait after failure of the database connection. This value is doubled on each failed attempt to reconnect, up to a maximum of MaxWaitReconnect.

### Password
Specifies the password string, which can include variables, used to specify a Bind prior to any search within a request. If this parameter is not specified, the packet’s password is used.

### Port
The TCP port of the LDAP server, or 0 to use the standard port. Default value is 0.

### QueryTimeout
Specifies the number of seconds to wait for the execution of an LDAP request to complete before timing out. This value is passed to the database engine, which may or may not implement the feature.

### Search
The value of this parameter is a string, name. The name specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same .aut file.

### SSL
- If set to 0, SSL is not used over the LDAP connection.
- If set to 1, SSL is used over the LDAP connection. Default value is 0.

### WaitReconnect
Specifies the number of seconds to wait after a failure of the database connection before trying to connect again.

---

### Table 135: *.aut [Server/name] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlashReconnect</td>
<td>If the server is down when performing a Bind or a Search, setting this parameter to 1 triggers a reconnection attempt before rejecting the request. Therefore, requests are not rejected due to inactivity timeouts. This setting applies to a particular server. To apply it for all servers, place it in the [Settings] section.</td>
</tr>
<tr>
<td>Host</td>
<td>The host name or IP address of the LDAP server.</td>
</tr>
<tr>
<td>LastResort</td>
<td>You may identify a “last resort” LDAP server by providing a LastResort parameter in one of these [Server/name] sections, and setting its value to 1. If an LDAP query against some other server results in “no record found,” the authentication server tries the last resort server before accepting or rejecting the user. You might use the LastResort parameter to identify your master accounts database. This enables Steel-Belted Radius to cover the case in which a user account is newly added but has not yet been propagated to all the LDAP databases.</td>
</tr>
<tr>
<td>LdapVersion</td>
<td>Specifies the version of LDAP protocol, if needed to override the default given in the [Settings] section.</td>
</tr>
<tr>
<td>MaxConcurrent</td>
<td>Specifies the maximum number of instances of a single LDAP request that may be executing at one time.</td>
</tr>
<tr>
<td>MaxWaitReconnect</td>
<td>Specifies the maximum number of seconds to wait after successive failures to reconnect after a failure of the database connection. WaitReconnect specifies the time to wait after failure of the database connection. This value is doubled on each failed attempt to reconnect, up to a maximum of MaxWaitReconnect.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password string, which can include variables, used to specify a Bind prior to any search within a request. If this parameter is not specified, the packet’s password is used.</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP port of the LDAP server, or 0 to use the standard port. Default value is 0.</td>
</tr>
<tr>
<td>QueryTimeout</td>
<td>Specifies the number of seconds to wait for the execution of an LDAP request to complete before timing out. This value is passed to the database engine, which may or may not implement the feature.</td>
</tr>
<tr>
<td>Search</td>
<td>The value of this parameter is a string, name. The name specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same .aut file.</td>
</tr>
<tr>
<td>SSL</td>
<td>- If set to 0, SSL is not used over the LDAP connection. - If set to 1, SSL is used over the LDAP connection. Default value is 0.</td>
</tr>
<tr>
<td>WaitReconnect</td>
<td>Specifies the number of seconds to wait after a failure of the database connection before trying to connect again.</td>
</tr>
</tbody>
</table>
[Server] Section

Used by: GEE, SPE, SPE + MIM, SPE + EAP, EE*
Not used by: —

Enterprise Edition

The [Server] section of the LDAP authentication header file lists the LDAP server used to perform authentication.

The syntax is as follows:

```
[Server]
  ServerName=TargetNumber
```

where ServerName is the name of the header file section that contains configuration information for that server, and TargetNumber is an activation target number, a number that controls when this server is activated for backup purposes. TargetNumber is optional and may be left blank. For example:

```
[Server]
s1 =
```

Global Enterprise Edition/Service Provider Edition

The [Server] section of the LDAP authentication header file lists the LDAP servers that may be used to perform authentication. If you are running the GEE or SPE edition of Steel-Belted Radius, you can specify more than one server in the [Server] section for load-balancing or backup. When more than one server is specified, Steel-Belted Radius authenticates against these databases in a round-robin fashion.

The syntax is as follows:

```
[Server]
  ServerName=TargetNumber
  ServerName=TargetNumber
```

where ServerName is the name of a header file section that contains configuration information for that server, and TargetNumber is an activation target number, a number that controls when this server is activated for backup purposes. TargetNumber is optional and may be left blank. For example:

```
[Server]
s1 =
s2 =

[Server/s1]
  ;Connection details for server s1

[Server/s2]
  ;Connection details for server s2
```
A Steel-Belted Radius server maintains connectivity with its LDAP servers according to the following rules:

- The priority of the server by order. The first entry in the [Server] section has the highest priority.
- By activation target number. The rule for the activation target is that if the number of LDAP servers that Steel-Belted Radius is connected to is less than the activation target, Steel-Belted Radius connects to the server and includes it in the round-robin list. While the number of active servers is equal to or greater that the activation target, Steel-Belted Radius does not use that server in the round-robin list. An activation target of 0 indicates that, in the current configuration, this machine is never used.

[Settings] Section

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP, EE*
**Not used by:** —

The [Settings] section of the LDAP authentication header file forms a basis for all Bind and Search requests to the LDAP database server(s).

Search sequencing is flexible. You can override search results using the $reject and $accept keywords.

**GEE/SPE:** You can proceed to a new search even if the current search returns no data by using the OnNotFound parameter.

For examples of using flexible searching, see “[Server/name] Sections” on page 261.

The parameters in the [Settings] section apply to all LDAP servers listed in the header file. The following parameters are usually present. If any of these parameters is not provided in the [Settings] section, the parameter assumes a system default value.

The values set in [Settings] for some parameters, such as ConnectTimeout, MaxConcurrent, or WaitReconnect, provide defaults that apply to all servers. These default values can be overridden for a particular server by entering the same parameter with a different value in a [Server/name] section.
Table 136: *.aut [Settings] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind</td>
<td>For Bind authentication, you must specify a Bind template in the [Settings] section of the LDAP authentication header file. The Bind template must follow conventional LDAP syntax. It may be as simple or as complex as LDAP syntax permits, with multiple attribute/value assertions in boolean combination. It may also include replacement variables from the Variable Table. Each replacement variable consists of the variable name enclosed in angle brackets (&lt;&gt;). Upon execution of the LDAP Bind request, the value of the variable replaces the variable name. For example, a Bind template that uses the User-Name attribute from the RADIUS request might look like this: uid=&lt;User-Name&gt;, ou=Special Users, o=bigco.com</td>
</tr>
<tr>
<td>BindName</td>
<td>For BindName authentication, you must omit the Bind parameter from the LDAP authentication header file. Use the BindName and BindPassword parameters instead. In the [Settings] section, BindName and BindPassword specify a default LDAP Bind template to use for all servers. You can also use BindName and BindPassword in [Server/name] sections to override this default for an individual server See “[Server/name] Sections” on page 261.</td>
</tr>
<tr>
<td>ConnectTimeout</td>
<td>Specifies the number of seconds to wait when attempting to establish the connection to the database before timing out. This value is passed to the client database engine, which may or may not implement the feature. Default value is 25 seconds. NOTE: The value specified in this parameter can be overridden in individual [Server/name] sections of this file.</td>
</tr>
<tr>
<td>LdapVersion</td>
<td>Specifies the version of LDAP protocol. Default value is 2.</td>
</tr>
<tr>
<td>LogLevel</td>
<td>Activates logging for the LDAP authentication component and sets the rate at which it writes entries to the Steel-Belted Radius server log file (.LOG). This value may be the number 0, 1, or 2, where 0 is the lowest logging level, 1 is intermediate, and 2 is the most verbose. If the LogLevel that you set in the .aut file is different than the LogLevel in radius.ini, the radius.ini setting determines the rate of logging. GEE/SPE: The LogLevel is re-read whenever the server receives a HUP signal.</td>
</tr>
</tbody>
</table>

FilterSpecial CharacterHandling
- If set to 1, specifies that non-alphanumeric characters, such as ( or ), should be converted to an ASCII hex value preceded by a backslash when they are encountered in a user name during authentication.
- If set to 0, non-alphanumeric characters are not converted during authentication. Default value is 0.

FlashReconnect If a server is down when performing a Bind or a Search, setting this parameter to 1 triggers a reconnection attempt before rejecting the request. Therefore, requests are not rejected due to inactivity timeouts. This setting applies to all servers. To apply it for a particular server, place it in the appropriate [Server/name] section.
### Table 136: *.aut [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxConcurrent</td>
<td>Specifies the maximum number of instances of a single LDAP request that may be executing at one time.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The value specified in this parameter can be overridden in individual [Server/name] sections of this file.</td>
</tr>
<tr>
<td>MaxScriptSteps</td>
<td>Specifies the maximum number of statements that a script can execute before terminating. You can use the MaxScriptSteps parameter to make sure a script does not get caught in an infinite loop.</td>
</tr>
<tr>
<td></td>
<td>Default value is 10000.</td>
</tr>
<tr>
<td>MaxWaitReconnect</td>
<td>Specifies the maximum number of seconds to wait after successive failures to reconnect after a failure of the database connection.</td>
</tr>
<tr>
<td></td>
<td>WaitReconnect specifies the time to wait after failure of the database connection. This value is doubled on each failed attempt to reconnect, up to a maximum of MaxWaitReconnect.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The value specified in this parameter can be overridden in individual [Server/name] sections of this file.</td>
</tr>
<tr>
<td>OnFound</td>
<td>Specifies the next request section when data is found. The value of this parameter is a string, <em>name</em>. The <em>name</em> specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same .aut file. If there is no next request section, the overall operation succeeds. This can be overridden using the $reject keyword, which causes the operation to fail when data is found.</td>
</tr>
<tr>
<td></td>
<td>(GEE/SPE only)</td>
</tr>
<tr>
<td>OnNotFound</td>
<td>Specifies the next request section when data is not found. The value of this parameter is a string, <em>name</em>. The <em>name</em> specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same .aut file. If there is no next request section, the overall operation fails. This can be overridden using the $accept keyword, which causes the operation to succeed when data is not found.</td>
</tr>
<tr>
<td></td>
<td>(GEE/SPE only)</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password string, which can include variables, used to specify a Bind prior to any search within a request. If this parameter is not specified, the packet’s password is used.</td>
</tr>
<tr>
<td>PasswordCase</td>
<td>■ If set to U or Upper, the password returned from the LDAP database is converted to uppercase before authentication.</td>
</tr>
<tr>
<td></td>
<td>■ If set to L or Lower, the password is converted to lowercase.</td>
</tr>
<tr>
<td></td>
<td>■ If set to O or Original, the password is not altered before authentication.</td>
</tr>
<tr>
<td></td>
<td>Default value is Original.</td>
</tr>
<tr>
<td>PasswordFormat</td>
<td>By default, the PasswordFormat parameter is not listed in the [Settings] section of the LDAP authentication header file. With no listing, Steel-Belted Radius expects the user's password in the LDAP table to be in cleartext format.</td>
</tr>
<tr>
<td></td>
<td>If you want to configure Steel-Belted Radius to automatically handle password values correctly when it detects that they have been encrypted using UNIXcrypt or a SHA1 + Base64 hash, set PasswordFormat to auto.</td>
</tr>
<tr>
<td>QueryTimeout</td>
<td>Specifies the timeout value in seconds for an individual search performed against the LDAP server.</td>
</tr>
<tr>
<td></td>
<td>Default value is 10 seconds.</td>
</tr>
</tbody>
</table>
### Table 136: *.aut [Settings] Syntax (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScriptTraceLevel</td>
<td>Specifies the level of detail for line-by-line script tracing in the log.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 0, no traces are logged.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, traces are only logged when the <code>SbrTrace()</code> function is executed by the script.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 2, a trace is generated for every line executed by the script.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>Search</td>
<td>Specifies an LDAP Search request by referencing a [Search/name] section elsewhere in the same *.aut file.</td>
</tr>
<tr>
<td>SSL</td>
<td>■ If set to 0, SSL is not used over the LDAP connection.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, SSL is used over the LDAP connection.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The value specified in this parameter can be overridden in individual [Server/name] sections of this file.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the maximum number of seconds for the overall timeout for each request, which includes the delay in acquiring resources, attempts against multiple LDAP servers, and so forth.</td>
</tr>
<tr>
<td></td>
<td>Default value is 20 seconds.</td>
</tr>
<tr>
<td>UpperCaseName</td>
<td>■ If set to 0, preserves the case of the username.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, converts the username to uppercase.</td>
</tr>
<tr>
<td></td>
<td>Default value is 0.</td>
</tr>
<tr>
<td>UTC</td>
<td>■ If set to 0, time values are displayed using the local time.</td>
</tr>
<tr>
<td></td>
<td>■ If set to 1, time values are displayed using universal time coordinates (UTC).</td>
</tr>
<tr>
<td>WaitReconnect</td>
<td>Specifies the number of seconds to wait after a failure of the database connection before trying to connect again.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The value specified in this parameter can be overridden in individual [Server/name] sections of this file.</td>
</tr>
</tbody>
</table>

### [Failure] Section

**Used by:** GEE, SPE, SPE + MIM, SPE + EAP  
**Not used by:** EE

The [Failure] section of the LDAP authentication header file (Table 137) can be used to determine the result of the authentication process (accept or reject) when connectivity to all of the configured LDAP databases has failed. For example:

```plaintext
[Failure]
Accept = 1
Profile = XYZ
FullName = Mr Stanley Smith
```

**NOTE:** The Profile option and the Alias option cannot be used together. Read the following descriptions and choose the one that suits your needs.
### Table 137: *.aut [Failure] Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
</table>
| Accept    | If set to 1, Steel-Belted Radius returns an Access-Accept packet with the Profile, FullName, and/or Alias attributes specified in the corresponding [Failure] section parameters.  
|           | If set to 0, the user is rejected. |
| Profile   | This is the name of an existing Steel-Belted Radius Profile entry, whose checklist and return list attributes are applied to the user’s connection. |
| FullName  | This string is the full user name, which is used in the Class attribute in the Access-Accept message. |
| Alias     | As an alternative to using the Profile parameter, you can use the Alias parameter to name an existing Steel-Belted Radius Native User entry. Steel-Belted Radius then applies the checklist and return list attributes of this User entry to the user’s connection.  
|           | **NOTE**: The Alias feature permits the Maximum Concurrent Connection limit (settable in the Users panel) to be applied to the user’s connection. |
|           | **Important**: You are strongly recommended to use Profile, as use of Alias has been deprecated. The LoginLimit value lets you implement the concurrent connection limits previously available through Alias. |
|           | If you want to apply concurrent connection limits to users who are being authenticated by means of LDAP, you must set up a Native User entry specifically for this purpose, with all of the appropriate checklist and return list attributes, and with no password. You can set up as many such accounts as you require. These entries store a specific set of checklist and return list attributes for LDAP authentication, for use only with the Alias parameter.  
|           | **NOTE**: Native User entries without passwords cannot be authenticated. This is a safety feature built into Steel-Belted Radius. Therefore, setting up User entries in preparation for using the Alias parameter with LDAP authentication does not pose a “back door” security risk. |
|           | **NOTE**: The Native User authentication method displayed in the Authentication Policies panel does not need to be activated for the Alias feature to work. |
Appendix A

Authentication Protocols

This appendix provides a matrix of authentication methods and their supported authentication protocols.

<table>
<thead>
<tr>
<th>Method</th>
<th>PAP</th>
<th>CHAP</th>
<th>MS-CHAP</th>
<th>MS-CHAP-V2</th>
<th>LEAP</th>
<th>EAP-MSCHAP-V2</th>
<th>EAP-MD5</th>
<th>PAP/Token card</th>
<th>EAP/Token card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft PEAP available inner authentication protocols</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Cisco PEAP available inner authentication protocols</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>TTLS available inner authentication protocols</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Native</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Native (password saved as Allow PAP only: {SHA} or {crypt}).</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Windows Domain Authentication

<table>
<thead>
<tr>
<th>Method</th>
<th>PAP</th>
<th>CHAP</th>
<th>MS-CHAP</th>
<th>MS-CHAP-V2</th>
<th>LEAP</th>
<th>EAP-MSCHAP-V2</th>
<th>EAP-MD5</th>
<th>PAP/Token card</th>
<th>EAP/Token card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Domain Group</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Windows Domain User</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Solaris authentication methods

<table>
<thead>
<tr>
<th>Method</th>
<th>PAP</th>
<th>CHAP</th>
<th>MS-CHAP</th>
<th>MS-CHAP-V2</th>
<th>LEAP</th>
<th>EAP-MSCHAP-V2</th>
<th>EAP-MD5</th>
<th>PAP/Token card</th>
<th>EAP/Token card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris User</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Solaris Group</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Other authentication plug-ins

<table>
<thead>
<tr>
<th>Method</th>
<th>PAP</th>
<th>CHAP</th>
<th>MS-CHAP</th>
<th>MS-CHAP-V2</th>
<th>LEAP</th>
<th>EAP-MSCHAP-V2</th>
<th>EAP-MD5</th>
<th>PAP/Token card</th>
<th>EAP/Token card</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurID</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

LDAP

<table>
<thead>
<tr>
<th>Method</th>
<th>PAP</th>
<th>CHAP</th>
<th>MS-CHAP</th>
<th>MS-CHAP-V2</th>
<th>LEAP</th>
<th>EAP-MSCHAP-V2</th>
<th>EAP-MD5</th>
<th>PAP/Token card</th>
<th>EAP/Token card</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIND (this includes AD and eDirectory/NDS)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>BINDNAME (password stored in clear text)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>BINDNAME (password stored in SHA/SolarisCrypt text)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>BINDNAME (password stored as MD4 hash of unicode value text)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
**Table 138: Authentication Protocols (continued)**

<table>
<thead>
<tr>
<th>Method</th>
<th>PAP</th>
<th>CHAP</th>
<th>MS-CHAP</th>
<th>MS-CHAP-V2</th>
<th>LEAP</th>
<th>EAP-MSCHAP-V2</th>
<th>EAP-MD5</th>
<th>PAP/Token card</th>
<th>EAP/Token card</th>
</tr>
</thead>
<tbody>
<tr>
<td>BINDNAME (password Stored as enc-md5)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SQL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password stored in clear text</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Password password stored in SHA/Solaris Crypt text</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Password stored as {MD4} hash of unicode value text</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Password stored as {enc-md5}</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Appendix B
Vendor-Specific Attributes

Table 139 describes the vendor-specific attributes used with core Steel-Belted Radius.

Table 139: Steel-Belted Radius Vendor-Specific Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funk-Allowed-Access-Hours</td>
<td>May be placed in the checklist for a user or profile entry to control the exact time periods during which a user may be allowed access. Funk-Allowed-Access-Hours is a variable-length string that identifies time periods in a 7-day week of 24-hour days. This string consists of one or more day specifiers (each of which may list one or more days and/or ranges of days) followed by one or more ranges of 24-hour times, in minutes.</td>
</tr>
<tr>
<td>Funk-Concurrent-Login-Limit</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>Funk-Full-User-Name</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>Funk-Location-Group-Id</td>
<td>Added to an inbound authentication or accounting request when the request is matched to a location group and AddFunkLocationGroupIdToRequest is set to 1 in the radius.ini file. The value of the attribute is the name of the location group.</td>
</tr>
<tr>
<td>Funk-Peer-Cert-Hash</td>
<td>Added to the list of attributes available for secondary authorization processing when EAP-TLS is loaded as an automatic EAP helper. The attribute is added to the request only if Include_Certificate_Info in the [Secondary_Authorization] section of tlsauth.eap is set to 1. The value of the attribute is the hexadecimal ASCII representation of the SHA1 hash of the client’s certificate.</td>
</tr>
<tr>
<td>Funk-Peer-Cert-Issuer</td>
<td>Added to the list of attributes available for secondary authorization processing when EAP-TLS is loaded as an automatic EAP helper. The attribute is added to the request only if Include_Certificate_Info in the [Secondary_Authorization] section of tlsauth.eap is set to 1. The value of the attribute is the contents of the Issuer attribute of the client’s certificate.</td>
</tr>
</tbody>
</table>
Table 139: Steel-Belted Radius Vendor-Specific Attributes (continued)

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funk-Peer-Cert-Principal</td>
<td>Added to the list of attributes available for secondary authorization processing when EAP-TLS is loaded as an automatic EAP helper. The attribute is added to the request only if Include_Certificate_Info in the [Secondary_Authorization] section of tlsauth.eap is set to 1. The value of the attribute is the contents of the Subject Alternate Name or Other Name attribute of the client’s certificate.</td>
</tr>
<tr>
<td>Funk-Peer-Cert-Subject</td>
<td>Added to the list of attributes available for secondary authorization processing when EAP-TLS is loaded as an automatic EAP helper. The attribute is added to the request only if Include_Certificate_Info in the [Secondary_Authorization] section of tlsauth.eap is set to 1. The value of the attribute is the contents of the Subject attribute of the client’s certificate.</td>
</tr>
<tr>
<td>Funk-Round-Robin-Group</td>
<td>May be placed in the return list for a user or profile entry to dynamically assign an attribute set from an Attribute Value Pool at log-in time. The value of this attribute must be set to the .rr file name which defines the Attribute Value Pool.</td>
</tr>
<tr>
<td>Funk-Source-IP-Address</td>
<td>Added to the list of attributes available for request processing if AddSourceIPAddressAttrToRequest is set to 1 in the [Configuration] section of the radius.ini file. The value of the attribute is the IP address from which the packet containing the request was received.</td>
</tr>
<tr>
<td>Funk-Source-IPv6-Address</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>Funk-Tribe-Name</td>
<td>Reserved for the Service Level Manager module to Steel-Belted Radius/Service Provider Edition.</td>
</tr>
</tbody>
</table>
Appendix C
SNMP Traps and Statistics

Steel-Belted Radius contains support for setting and retrieving configuration information via standard SNMP utilities. This appendix summarizes the proprietary SNMP traps and rate statistics generated by Steel-Belted Radius.

- The fnkradtr.mib MIB defines the content of the traps that are generated by the Steel-Belted Radius server for SNMPv1.
- The fnkradtr-v2.mib MIB defines the content of the traps that are generated by the Steel-Belted Radius server for SNMPv2.
- The fnkrate.mib MIB defines the peak, current, and average rate statistics maintained by Steel-Belted Radius.

NOTE: The SNMP subagent in Steel-Belted Radius may generate traps that do not reference Funk enterprise IDs. For information on generic SNMP traps specified by IETF-specified MIBs, refer to the appropriate RFC. For information on generic netSnmp traps specified by netSnmp-specific MIBs, refer to the netSnmp documentation.
## Trap Variables

Table 140 lists the trap variables for the proprietary SNMP traps used by Steel-Belted Radius.

### Table 140: Trap Variables

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Identifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>funkSbrTrapVarComp</td>
<td>The component within the SBR server that issued the trap.</td>
</tr>
<tr>
<td></td>
<td>1 – Core</td>
</tr>
<tr>
<td></td>
<td>2 – Accounting</td>
</tr>
<tr>
<td></td>
<td>3 – Authentication</td>
</tr>
<tr>
<td>funkSbrTrapVarSev</td>
<td>The severity of the event that caused the trap.</td>
</tr>
<tr>
<td></td>
<td>1 – Informational</td>
</tr>
<tr>
<td></td>
<td>2 – Warning</td>
</tr>
<tr>
<td></td>
<td>3 – Error</td>
</tr>
<tr>
<td>funkSbrTrapVarSWName</td>
<td>The identity of the software that is the RADIUS server.</td>
</tr>
<tr>
<td>funkSbrTrapVarThreadsAvail</td>
<td>The number of threads available in the thread worker pool.</td>
</tr>
<tr>
<td>funkSbrTrapVarBytesAvail</td>
<td>The number of bytes available in the file system.</td>
</tr>
<tr>
<td>funkSbrTrapVarPrivateDir</td>
<td>The file system path to the private directory used by the RADIUS server.</td>
</tr>
<tr>
<td>funkSbrTrapVarNumberOfOccurrences</td>
<td>The dilution factor for the trap. The trap is sent on once for every 'n' occurrences of this event.</td>
</tr>
<tr>
<td>funkSbrTrapVarSQLConnects</td>
<td>The number of connection attempts to a SQL database.</td>
</tr>
<tr>
<td>funkSbrTrapVarSQLDisconnects</td>
<td>The number of disconnects from a SQL database (due to an error encountered during an operation).</td>
</tr>
<tr>
<td>funkSbrTrapVarSQLTimeouts</td>
<td>The number of timeouts encountered when trying to perform a transaction against a SQL database.</td>
</tr>
<tr>
<td>funkSbrTrapVarServiceDispatcherErrCode</td>
<td>The error code returned in response to an attempt to start the RADIUS service on Windows.</td>
</tr>
<tr>
<td>funkSbrTrapVarSetStatusErrCode</td>
<td>The error code returned in response to an attempt to inform the service control dispatcher of the status of the RADIUS service on Windows.</td>
</tr>
<tr>
<td>funkSbrTrapVarGetDiskFreeSpaceErrCode</td>
<td>The error code returned in response to an attempt to call GetDiskFreeSpaceEx to determine the amount of free disk space available on Windows.</td>
</tr>
<tr>
<td>funkSbrTrapVarIniString</td>
<td>The .ini file setting used to specify a configuration value.</td>
</tr>
<tr>
<td>funkSbrTrapVarDbType</td>
<td>The type of database being employed by the RADIUS server.</td>
</tr>
<tr>
<td>funkSbrTrapVarFailedSystemName</td>
<td>The name of the remote system failing connectivity from the RADIUS server.</td>
</tr>
<tr>
<td>funkSbrTrapVarUserName</td>
<td>The name of the user to whom the trap refers.</td>
</tr>
<tr>
<td>funkSbrTrapVarPersistStoreName</td>
<td>The name of the persistent storage to which the trap refers.</td>
</tr>
</tbody>
</table>
Table 140: Trap Variables (continued)

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Identifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>funkSbrTrapVarDiagnosticMessage</td>
<td>A generic diagnostic message that may be helpful in determining and addressing the possible root causes of the trap.</td>
</tr>
<tr>
<td>funkSbrTrapVarIPAddrPoolName</td>
<td>The name of the IP address pool to which the trap refers.</td>
</tr>
<tr>
<td>funkSbrTrapVarIPAddrAvail</td>
<td>The number of addresses available in the IP address pool.</td>
</tr>
<tr>
<td>funkSbrTrapVarConnectedSystemName</td>
<td>The name of the remote system with which the RADIUS server has established a connection.</td>
</tr>
<tr>
<td>funkSbrTrapVarQueueName</td>
<td>The name of a queue in the RADIUS server. Implemented in Steel-Belted Radius version 5.3</td>
</tr>
</tbody>
</table>
Trap Definitions

Table 141 lists proprietary SNMP traps generated by Steel-Belted Radius. The columns in Table 141 consist of the following:

- OID Suffix – Identifies the OID suffix for the trap. To identify the OID number for an alarm, append the OID suffix to the Funk OID prefix (1.3.6.1.4.1.1411). For example, the ASN.1 number for the `funkSbrTrapServiceStarted` trap is 1.3.6.1.4.1.1411.100.

- Trap – Identifies the name of the proprietary trap.

- Description – Describes when the trap is generated.

- Type – Indicates whether the trap is informational, warning, or error

- Added to SBR – Identifies the version of Steel-Belted Radius in which the trap first appeared.

**NOTE:** Some Steel-Belted Radius traps are dilutable, which means that one trap message is generated after a specified number of events of that type occur.

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>funkSbrTrapServiceStarted</td>
<td>Sent when the RADIUS server is started.</td>
<td>Info</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cause:</strong> Trap indicates that the server itself has started. This does not mean that all of the various configured features have loaded successfully. If there is an issue with another component, traps specific to it will indicate so. This trap will show that a valid license is installed. It is now possible to interact with the server through the SBR Administrator or the LDAP Configuration Interface. <strong>Severity:</strong> If unexpected, this could be the result of a core in the <code>radius</code> process.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>funkSbrTrapServiceStopped</td>
<td>Sent when the RADIUS server is stopped.</td>
<td>Info</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cause:</strong> The server completed its shutdown operation and is no longer running. Server will not respond to any operation from the SBR Administrator, from the LCI, or from any inbound RADIUS data. <strong>Severity:</strong> If unexpected, this could be the result of a core in the radius process.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 141: fnkradtr.mib Trap Definitions (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>102</td>
<td>funkSbrTrapThreadsNormal</td>
<td>Sent when the number of available threads in the accounting or authentication server has risen above a specified threshold.</td>
<td>Info</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cause:</strong> The number of available threads on the system has risen above the threshold configured in the <code>events.ini</code> file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Severity:</strong> Could result in loss of packets or inoperability.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103</td>
<td>funkSbrTrapFSNormal</td>
<td>Sent when the number of bytes available in the file system from which the server is running has risen above a specified threshold.</td>
<td>Info</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cause:</strong> The number of bytes available in the free disk space has increased above the threshold configured in the <code>events.ini</code> file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Severity:</strong> This can cause the system to become inoperable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>funkSbrTrapConcurrencyReconnect</td>
<td>Sent when RADIUS reconnects to the Service Level Manager server after it has sent a ConcurrencyFailure, ConcurrencyTimeout, or ConcurrencyLocalProxyFailure trap.</td>
<td>Info</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cause:</strong> If a failure to communicate with the Concurrency Server has occurred, this trap is sent when communications have been re-established and the SLM server is responding again.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Severity:</strong> Users may have either been rejected, or they may have been able to exceed their configured concurrent login policy, during the time interval when communications with the CS were down. This will depend on the settings in the forward.aut configuration file which resides on any of the SBR servers acting as clients to the CS. Check the RejectIfUnreachable setting if you are uncertain as to the expected behavior of SBR in the event that the CS is unreachable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>funkSbrTrapSQLReconnect</td>
<td>Sent when Radius reconnects to the SQL database after it has sent a SQLConnectFail trap.</td>
<td>Info</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Cause:</strong> If a failure to communicate with the SQL server database has occurred, this trap is sent when communications have been re-established and the SQL server is responding again.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Severity:</strong> Users may have either been rejected, or they may have been allowed onto the network without proper verification of credentials, during the time interval when the SQL server was unreachable. This will depend on the settings in the <code>radsql.aut</code> configuration file. Check the [Failure] section settings if you are uncertain as to the expected behavior of Steel-Belted Radius in the event that the SQL server is unreachable.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 141: fnkradtr.mib Trap Definitions (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
</table>
| 106        | funkSbrTrapLDAPReconnect           | Sent when Radius reconnects to the LDAP server after it has sent a LDAPConnectFail trap.  
**Cause:** If a failure to communicate with the LDAP database has occurred, this trap is sent when communications have been re-established and the LDAP server is responding again.  
**Severity:** Users may have either been rejected, or they may have been allowed onto the network without proper verification of credentials, during the time interval when the LDAP server was unreachable. This will depend on the settings in the ldapauth.aut configuration file. Check the [Failure] section settings if you are uncertain as to the expected behavior of SBR in the event that the LDAP database is unreachable. | Info 1.15 |
| 107        | funkSbrTrapUserAccountLocked       | Sent when a user’s account becomes locked out due to an excessive number of rejected authentication attempts within a defined period of time.  
**Cause:** A user's account is locked, disallowing access to the network, after an excessive number of rejected authentication attempts. This functionality is configured in the lockout.ini file.  
**Severity:** The user will not be able to access the network until the account is unlocked. | Info 1.15 |
| 108        | funkSbrTrapUserAccountReleased     | Sent when a user's account, previously locked due to an excessive number of rejected authentication attempts, becomes unlocked. | Info 1.15 |
| 109        | funkSbrTrapProxySpoolReconnect     | Sent when the proxy accounting spooler reconnects to the target realm after it has sent a ProxySpoolTimeout trap.  
**Cause:** Issues affecting transmission of spooled accounting proxy data to the configured downstream target(s) have been resolved (possibly a restoration of the network link, or the downstream proxy accounting server has become available again).  
**Severity:** If unexpected, then the accounting target system (possibly a billing server) was not receiving data from the AAA server for some time interval. During that time, data was written to the local disk for temporary storage until the accounting target became available again. There should be no data lost. | Info 1.15 |
| 110        | funkSbrTrapiPAaddrPoolNormal       | Sent when the number of available IP addresses in any pool rises above a specified threshold. IP pool thresholds can be configured in events.ini file.  
**Severity:** Users could have been rejected if threshold warning trap 5027 was ignored. | Info 1.15 |
| 111        | funkSbrTrapSQLConnect              | Sent only once, when Radius initially connects to the SQL database. | Info 4.04 |
| 112        | funkSbrTrapLDAPConnect             | Sent only once, when Radius initially connects to the LDAP server. | Info 4.04 |
| 113        | funkSbrTrapWatchdogStarted         | Sent when the radiusd watchdog is started. | Info 4.04 |
## Table 141: fnkradtr.mib Trap Definitions (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>114</td>
<td>funkSbrTrapWatchdogStopped</td>
<td>Sent when the radiusd watchdog is stopped.</td>
<td>Info</td>
<td>4.04</td>
</tr>
<tr>
<td>115</td>
<td>funkSbrTrapWatchdogRadiusStarted</td>
<td>Sent whenever the radiusd watchdog attempts to (re)start the RADIUS server.</td>
<td>Info</td>
<td>4.04</td>
</tr>
<tr>
<td>116</td>
<td>funkSbrTrapWatchdogRadiusStopped</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>117</td>
<td>funkSbrTrapUserAccountRedirected</td>
<td>Sent when a user account has been redirected due to an excessive number of rejected authentication attempts.</td>
<td>Info</td>
<td>5.3</td>
</tr>
<tr>
<td>118</td>
<td>funkSbrTrapSS7CommunicationOK</td>
<td>Sent when SS7 communications are successful after a funkSbrTrapSS7CommunicationError trap has been sent.</td>
<td>Info</td>
<td>5.3</td>
</tr>
<tr>
<td>119</td>
<td>funkSbrTrapSS7CDRGenerationOK</td>
<td>Sent when CDR generation is successful after a funkSbrTrapSS7CDRGenerationError trap has been sent.</td>
<td>Info</td>
<td>5.3</td>
</tr>
<tr>
<td>120</td>
<td>funkSbrTrapSS7AuthDatabaseOK</td>
<td>Sent when access to the Authorization databases are successful after a funkSbrTrapSS7AuthDatabaseError trap has been sent.</td>
<td>Info</td>
<td>5.3</td>
</tr>
<tr>
<td>120</td>
<td>funkSbrTrapSS7ProvDatabaseOK</td>
<td>Sent when access to the SMS Provisioning database is successful after a funkSbrTrapSS7ProvDatabaseError trap has been sent.</td>
<td>Info</td>
<td>5.3</td>
</tr>
<tr>
<td>5000</td>
<td>funkSbrTrapCmdArgBadPrivDir</td>
<td>Sent when an invalid private directory is specified on the command line used to launch the RADIUS server. The command line option is ignored.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5001</td>
<td>funkSbrTrapLowThreads</td>
<td>Sent when the count of threads available for the accounting or authentication server drops below a configurable threshold. An informational trap is sent when the count of available threads (at some future point) rises to an acceptable level.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5002</td>
<td>funkSbrTrapConcurrencyFailure</td>
<td>Sent when communications with the RADIUS concurrency server fails. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5003</td>
<td>funkSbrTrapConcurrencyTimeout</td>
<td>Sent when communications with the RADIUS concurrency server times out. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5004</td>
<td>funkSbrTrapConcurrencyLocalProxyFailure</td>
<td>Sent when a local error prevents the RADIUS server from sending a proxy request to the RADIUS concurrency server. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5004</td>
<td>funkSbrTrapConcurrencyLocalProxyFailure</td>
<td>Sent when a local error prevents the RADIUS server from sending a proxy request to the RADIUS concurrency server. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5005</td>
<td>funkSbrTrapStaticAcctProxyTimeout</td>
<td>Sent when the RADIUS server times out in an attempt to forward an accounting request to the location specified by the static proxy option. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5006</td>
<td>funkSbrTrapStaticAcctProxyLocalFailure</td>
<td>Sent when the RADIUS server encounters a local failure in an attempt to forward an accounting request to the location specified by the static proxy option. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>OID Suffix</td>
<td>Trap Name</td>
<td>Description</td>
<td>Type</td>
<td>Added to SBR</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>5007</td>
<td>funkSbrTrapLowFSSpace</td>
<td>Sent when the amount of space available in the file system in which the server’s private directory resides falls below a configurable threshold. An informational trap is sent when the amount of available space (at some future point) rises to an acceptable level.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5008</td>
<td>funkSbrTrapSQLConnectFail</td>
<td>Sent when the connection to a SQL database has failed. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5009</td>
<td>funkSbrTrapSQLDisconnect</td>
<td>Sent when a disconnect to a SQL database occurs. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5010</td>
<td>funkSbrTrapSQLTimeout</td>
<td>Sent when a timeout occurs during an attempt to perform transactions to a SQL database. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5011</td>
<td>funkSbrTrapAcctDbTimeout</td>
<td>Sent when the access to the accounting database has timed out. Trap can be diluted. No longer supported.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5012</td>
<td>funkSbrTrapAcctDbFailure</td>
<td>Sent when the access to the accounting database has failed. Trap can be diluted. No longer supported.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5013</td>
<td>funkSbrTrapVerifyServerTimeout</td>
<td>Sent when an attempt to communicate with the Verification Server has timed out. Trap can be diluted. No longer supported.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5014</td>
<td>funkSbrTrapVerifyServerFail</td>
<td>Sent when an attempt to communicate with the Verification Server has failed. Trap can be diluted. No longer supported.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5015</td>
<td>funkSbrTrapLDAPConnectFailure</td>
<td>Sent when a connect failure to an LDAP server occurs. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5016</td>
<td>funkSbrTrapLDAPConnectFailures</td>
<td>Sent when an attempt to communicate with the LDAP Server has failed. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5017</td>
<td>funkSbrTrapLDAPDisconnect</td>
<td>Sent when the LDAP Server has disconnected. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5018</td>
<td>funkSbrTrapLDAPRequestTimeouts</td>
<td>Sent when a request sent to the LDAP Server has timed out. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5019</td>
<td>funkSbrTrapLDAPDisconnect</td>
<td>Sent when a disconnect to a LDAP server occurs. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5020</td>
<td>funkSbrTrapLDAPRequestTimeout</td>
<td>Sent when a request sent to the LDAP Server has timed out. Trap can be diluted.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
</tbody>
</table>
Table 141: fnkradtr.mib Trap Definitions (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>5021</td>
<td>funkSbrTrapProxySpoolTimeout</td>
<td>Sent when a request forwarded by the proxy accounting spooler has timed out.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5022</td>
<td>funkSbrTrapProxySpoolTimeouts</td>
<td>Sent when a request forwarded by the proxy accounting spooler has timed out.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5023</td>
<td>funkSbrTrapSoftLimitViolation</td>
<td>Sent when accepting a concurrency request exceeds a realm’s soft limit.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap can be diluted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5024</td>
<td>funkSbrTrapHardLimitViolation</td>
<td>Sent when a concurrency request is rejected because a realm’s hard limit has been reached.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap can be diluted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5025</td>
<td>funkSbrTrapConcurrencyServer Misconfiguration</td>
<td>Sent when a PAS realm has been misconfigured. All authentication requests to the named realm will be rejected.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5026</td>
<td>funkSbrTrapACCTWriteFailure</td>
<td>Sent when the server is unable to commit accounting data to a persistent store such as the file system, database, etc.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap can be diluted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5027</td>
<td>funkSbrTrapIPAddrPoolLow</td>
<td>Sent when the number of available IP addresses in any pool falls below a configurable threshold. An informational trap is sent when the number of available IP addresses (at some future point) rises to an acceptable level.</td>
<td>Warning</td>
<td>1.15</td>
</tr>
<tr>
<td>5028</td>
<td>funkSbrTrapWatchdogRadiusTerm</td>
<td>Sent whenever the radiusd watchdog attempts to send a TERM signal to terminate the RADIUS server.</td>
<td>Warning</td>
<td>4.04</td>
</tr>
<tr>
<td>5029</td>
<td>funkSbrTrapWatchdogRadiusKill</td>
<td>Sent whenever the radiusd watchdog attempts to send a KILL signal to terminate the RADIUS server.</td>
<td>Warning</td>
<td>4.04</td>
</tr>
<tr>
<td>5030</td>
<td>funkSbrTrapFloodQueueOverflow</td>
<td>Sent whenever a flood queue drops a packet.</td>
<td>Warning</td>
<td>5.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap can be diluted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5031</td>
<td>funkSbrTrapFailEAlni</td>
<td>Sent when an attempt to process the ea.ini file at server startup fails.</td>
<td>Warning</td>
<td>5.3</td>
</tr>
<tr>
<td>5032</td>
<td>funkSbrTrapPasError</td>
<td>Sent when rejecting a concurrency request for internal processing reasons.</td>
<td>Warning</td>
<td>6.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap can be diluted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5033</td>
<td>funkSbrTrapMappingFailure</td>
<td>Sent when rejecting a concurrency request that fails to resolve a realm or region name</td>
<td>Warning</td>
<td>6.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap can be diluted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5034</td>
<td>funkSbrTrapSubscriberLimitViolation</td>
<td>Sent when rejecting a concurrency request that exceeds a subscriber limit.</td>
<td>Warning</td>
<td>6.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap can be diluted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10000</td>
<td>funkSbrTrapStartServiceError</td>
<td>Sent for a Windows version of RADIUS when the service control dispatcher returns an error. Not used for SNMP on Solaris/Linux.</td>
<td>Error</td>
<td>1.15</td>
</tr>
</tbody>
</table>
### Table 141: fnkradtr.mib Trap Definitions (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>10001</td>
<td>funkSbrTrapSetStatusError</td>
<td>Sent for a Windows version of RADIUS when the attempt to inform the service control dispatcher of the status of the RADIUS server encounters an error. Not used for SNMP on Solaris/Linux.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10002</td>
<td>funkSbrTrapBadPrivDir</td>
<td>Sent for a Windows version of RADIUS when the attempt to inform the service control dispatcher of the status of the RADIUS server encounters an error. Not used for SNMP on Solaris/Linux.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10003</td>
<td>funkSbrTrapFailedThreadCreate</td>
<td>Sent when an attempt to create a thread at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10004</td>
<td>funkSbrTrapFailedMutexCreate</td>
<td>Sent when an attempt to create a mutual exclusion lock (mutex) at server startup encounters a failure. A mutex prevents multiple threads from executing critical sections of code simultaneously. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10005</td>
<td>funkSbrTrapFailedSignalInit</td>
<td>Sent when an attempt to initialize signal handling at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10006</td>
<td>funkSbrTrapFailedEventInit</td>
<td>Sent for a Windows version of RADIUS when an attempt to initialize event processing at server startup encounters a failure. The server will fail to start. Not used for SNMP on Solaris/Linux.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10007</td>
<td>funkSbrTrapFailedLogFile</td>
<td>Sent when an attempt to open or create a log file at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10008</td>
<td>funkSbrTrapFailedLDAPAdminInit</td>
<td>Sent when an attempt to initialize the LDAP administration interface at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10009</td>
<td>funkSbrTrapFailedRPCInit</td>
<td>Sent when an attempt to initialize the RPC administration interface at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10010</td>
<td>funkSbrTrapFailedIPInit</td>
<td>Sent when an attempt to initialize basic TCP/IP services at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10011</td>
<td>funkSbrTrapFailedCurrentSessionsInit</td>
<td>Sent when an attempt to initialize current sessions table processing at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10012</td>
<td>funkSbrTrapFailedChallCacheInit</td>
<td>Sent when an attempt to initialize the RADIUS challenge continuation cache at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10013</td>
<td>funkSbrTrapFailedActiveRASInit</td>
<td>Sent when an attempt to initialize the network access device activity monitor at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10014</td>
<td>funkSbrTrapFailedDictionaryInit</td>
<td>Sent when an attempt to initialize the dictionary processing at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
</tbody>
</table>
### Table 141: fnkradtr.mib Trap Definitions (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>10015</td>
<td>funkSbrTrapFailedVendorInit</td>
<td>Sent when an attempt to process the vendor.ini file at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10016</td>
<td>funkSbrTrapFailedDBInit</td>
<td>Sent when an attempt to initialize the internal database at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10017</td>
<td>funkSbrTrapFailedUnixUserInit</td>
<td>Sent when an attempt to initialize the Unix user browsing component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10018</td>
<td>funkSbrTrapFailedAdminRightsInit</td>
<td>Sent when an attempt to initialize the administration user rights component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10019</td>
<td>funkSbrTrapFailedDbOpen</td>
<td>Sent when an attempt to open the internal database at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10020</td>
<td>funkSbrTrapFailedDNISLookupInit</td>
<td>Sent when an attempt to initialize the tunnel DNIS lookup component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10021</td>
<td>funkSbrTrapFailedConfigCacheInit</td>
<td>Sent when an attempt to initialize the configuration caching component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10022</td>
<td>funkSbrTrapFailedDbCacheInit</td>
<td>Sent when an attempt to initialize the database caching component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10023</td>
<td>funkSbrTrapFailedLicenseInit</td>
<td>Sent when an attempt to initialize the licensing component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10024</td>
<td>funkSbrTrapFailedNDSTrusteeInit</td>
<td>Sent when an attempt to initialize NDS trustee processing on NetWare at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10025</td>
<td>funkSbrTrapFailedHostLookupInit</td>
<td>Sent when an attempt to initialize host lookup processing on NetWare at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10026</td>
<td>funkSbrTrapFailedAddrPoolInit</td>
<td>Sent when an attempt to initialize IP/IPX address pool resource management at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10027</td>
<td>funkSbrTrapFailedLoginLimitInit</td>
<td>Sent when an attempt to initialize user login count tracking at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10028</td>
<td>funkSbrTrapFailedPersistStoreCreate</td>
<td>Sent when an attempt to create the persistent store for current session list processing at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10029</td>
<td>funkSbrTrapFailedPersistStoreInit</td>
<td>Sent when an attempt to initialize the persistent store for current session list processing at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
</tbody>
</table>
Table 141: fnkradtr.mib Trap Definitions (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Trap Name</th>
<th>Description</th>
<th>Type</th>
<th>Added to SBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>10030</td>
<td>funkSbrTrapFailedPerfMonInit</td>
<td>Sent for a Windows version of RADIUS when an attempt to initialize the Windows performance monitor interface at server startup encounters a failure. The server will fail to start. Not used for SNMP on Solaris/Linux.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10031</td>
<td>funkSbrTrapFailedLockInit</td>
<td>Sent when an attempt to initialize admin locking component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10032</td>
<td>funkSbrTrapFailedPlugInInit</td>
<td>Sent when an attempt to initialize the plug-in support component at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10033</td>
<td>funkSbrTrapFailedPacketCacheInit</td>
<td>Sent when an attempt to initialize duplicate packet request cache at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10034</td>
<td>funkSbrTrapFailedNameMangleInit</td>
<td>Sent when an attempt to initialize name mangling support at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10035</td>
<td>funkSbrTrapFailedNameStripInit</td>
<td>Sent when an attempt to initialize name stripping support at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10036</td>
<td>funkSbrTrapFailedFSSpaceChecking</td>
<td>Sent when an attempt to determine the amount of free file system space fails. File system space checking will be disabled until the server is restarted.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10037</td>
<td>funkSbrTrapFailedNameValidateInit</td>
<td>Sent when an attempt to initialize name validation support at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10038</td>
<td>funkSbrTrapFailedResourceCheckInit</td>
<td>Sent when an attempt to initialize system resource checking at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10039</td>
<td>funkSbrTrapFailedSystemStatsInit</td>
<td>Sent when an attempt to initialize statistic collection at server startup encounters a failure. The server will fail to start.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10040</td>
<td>funkSbrTrapSQLConnectFailure</td>
<td>Sent when a connection attempt from the SQL authentication or accounting plug-in to the specified system has failed.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10041</td>
<td>funkSbrTrapSQLDiscon</td>
<td>Sent when a disconnect from a SQL database has occurred.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10042</td>
<td>* individual SQL timeout (not sent as a trap)</td>
<td>Sent when an attempt to allocate reserved memory based on a setting in the radius.ini file fails. The server will start without reserved memory, but will be unable to warn of low memory conditions.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10043</td>
<td>funkSbrTrapFailed Reserve Memory Alloc</td>
<td>Sent when an attempt to allocate memory during runtime fails and the block of memory reserved at system startup is freed in an attempt to alleviate the low memory condition.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10044</td>
<td>funkSbrTrapReserve Memory Freed</td>
<td>Sent when an attempt to allocate memory has failed and the block of memory reserved at system startup is freed in an attempt to alleviate the low memory condition.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>10045</td>
<td>funkSbrTrapMemory Alloc Fail</td>
<td>Sent when an attempt to allocate memory has failed. Trap can be diluted.</td>
<td>Error</td>
<td>1.15</td>
</tr>
<tr>
<td>OID Suffix</td>
<td>Trap Name</td>
<td>Description</td>
<td>Type</td>
<td>Added to SBR</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>--------------</td>
</tr>
<tr>
<td>10046</td>
<td>* individual accounting database connect failure (not sent as a trap)</td>
<td></td>
<td>Error 1.15</td>
<td></td>
</tr>
<tr>
<td>10047</td>
<td>* individual verification server connect failure (not sent as a trap)</td>
<td></td>
<td>Error 1.15</td>
<td></td>
</tr>
<tr>
<td>10048</td>
<td>funkSbrTrapFailedMibInfoCollectInit</td>
<td>Sent when an attempt to initialize MIB information collection at server startup encounters a failure. The server will fail to start.</td>
<td>Error 1.15</td>
<td></td>
</tr>
<tr>
<td>10049</td>
<td>funkSbrTrapFailedMibInfoAccessInit</td>
<td>Sent when an attempt to initialize MIB access at server startup encounters a failure. The server will fail to start.</td>
<td>Error 1.15</td>
<td></td>
</tr>
<tr>
<td>10050</td>
<td>funkSbrTrapFailedCommonIPInit</td>
<td>Sent when an attempt to initialize common IP services at server startup encounters a failure. The server will fail to start.</td>
<td>Error 1.15</td>
<td></td>
</tr>
<tr>
<td>10051</td>
<td>funkSbrTrapWatchdogAborted</td>
<td>Sent whenever the radiusd watchdog aborts. This is typically due to a prolonged inability to control or communicate with the RADIUS server, or some fatal error that has occurred within the watchdog itself.</td>
<td>Error 4.04</td>
<td></td>
</tr>
<tr>
<td>10052</td>
<td>funkSbrTrapWatchdogFailedInit</td>
<td>Sent whenever the radiusd watchdog is unable to initialize itself. This is typically due to insufficient or invalid command line parameters given to the watchdog itself.</td>
<td>Error 4.04</td>
<td></td>
</tr>
<tr>
<td>10053</td>
<td>funkSbrTrapAdminAuthFailedInit</td>
<td>Sent whenever the server is unable to initialize administrative authentication and authorization. The server will fail to start.</td>
<td>Error 5.3</td>
<td></td>
</tr>
<tr>
<td>10054</td>
<td>funkSbrTrapServiceFailedInit</td>
<td>Sent when the server has failed to start. This trap is sent in addition to a specific failure trap.</td>
<td>Error 5.3</td>
<td></td>
</tr>
<tr>
<td>10055</td>
<td>funkSbrTrapSS7MapGatewayFailedInit</td>
<td>Sent when the SS7 MAP Gateway has failed to initialize. The server will start but SS7 functions will not be available.</td>
<td>Error 5.3</td>
<td></td>
</tr>
<tr>
<td>10056</td>
<td>funkSbrTrapSS7CommunicationError</td>
<td>Sent when SS7 communication has failed.</td>
<td>Error 5.3</td>
<td></td>
</tr>
<tr>
<td>10057</td>
<td>funkSbrTrapSS7CDRGenerationError</td>
<td>Sent when CDRs cannot be written.</td>
<td>Error 5.3</td>
<td></td>
</tr>
<tr>
<td>10058</td>
<td>funkSbrTrapSS7AuthDatabaseError</td>
<td>Sent when access to an Authorization database has failed.</td>
<td>Error 5.3</td>
<td></td>
</tr>
<tr>
<td>10059</td>
<td>funkSbrTrapSS7ProvDatabaseError</td>
<td>Sent when access to the Provisioning database has failed.</td>
<td>Error 5.3</td>
<td></td>
</tr>
</tbody>
</table>
Server Rate Statistics

This section presents an overview of the SNMP accessible rate statistics maintained by Steel-Belted Radius.

The fnkrate.mib MIB maintains rate statistics for the Steel-Belted Radius server. Steel-Belted Radius maintains three types of values for these types of statistics:

- The current-rate statistics specify the rate measured over the most recent rate interval.
- The average-rate statistics specify the rate measured since startup, or the most recent statistics reset command.
- The peak-rate statistics specify the highest rate observed since startup, or the most recent statistics reset command.

Table 142: Server Rate Statistics

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Statistic</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>funkSbrRatesSecondsPerInterval</td>
<td>Specifies the duration (in seconds) of the interval over which the rate statistics are gathered.</td>
</tr>
<tr>
<td>2</td>
<td>funkSbrRatesAuthRequestCurrentRate</td>
<td>AuthRequest Current Rate</td>
</tr>
<tr>
<td>3</td>
<td>funkSbrRatesAuthRequestAverageRate</td>
<td>AuthRequest Average Rate</td>
</tr>
<tr>
<td>4</td>
<td>funkSbrRatesAuthRequestPeakRate</td>
<td>AuthRequest Peak Rate</td>
</tr>
<tr>
<td>5</td>
<td>funkSbrRatesAuthAcceptCurrentRate</td>
<td>AuthAccept Current Rate</td>
</tr>
<tr>
<td>6</td>
<td>funkSbrRatesAuthAcceptAverageRate</td>
<td>AuthAccept Average Rate</td>
</tr>
<tr>
<td>7</td>
<td>funkSbrRatesAuthAcceptPeakRate</td>
<td>AuthAccept Peak Rate</td>
</tr>
<tr>
<td>8</td>
<td>funkSbrRatesAuthRejectCurrentRate</td>
<td>AuthReject Current Rate</td>
</tr>
<tr>
<td>9</td>
<td>funkSbrRatesAuthRejectAverageRate</td>
<td>AuthReject Average Rate</td>
</tr>
<tr>
<td>10</td>
<td>funkSbrRatesAuthRejectPeakRate</td>
<td>AuthReject Peak Rate</td>
</tr>
<tr>
<td>11</td>
<td>funkSbrRatesAcctStartCurrentRate</td>
<td>AcctStart Current Rate</td>
</tr>
<tr>
<td>12</td>
<td>funkSbrRatesAcctStartAverageRate</td>
<td>AcctStart Average Rate</td>
</tr>
<tr>
<td>13</td>
<td>funkSbrRatesAcctStartPeakRate</td>
<td>AcctStart Peak Rate</td>
</tr>
<tr>
<td>14</td>
<td>funkSbrRatesAcctStopCurrentRate</td>
<td>AcctStop Current Rate</td>
</tr>
<tr>
<td>15</td>
<td>funkSbrRatesAcctStopAverageRate</td>
<td>AcctStop Average Rate</td>
</tr>
<tr>
<td>16</td>
<td>funkSbrRatesAcctStopPeakRate</td>
<td>AcctStop Peak Rate</td>
</tr>
<tr>
<td>17</td>
<td>funkSbrRatesProxyAuthRequestCurrentRate</td>
<td>ProxyAuthRequest Current Rate</td>
</tr>
<tr>
<td>18</td>
<td>funkSbrRatesProxyAuthRequestAverageRate</td>
<td>ProxyAuthRequest Average Rate</td>
</tr>
<tr>
<td>19</td>
<td>funkSbrRatesProxyAuthRequestPeakRate</td>
<td>ProxyAuthRequest Peak Rate</td>
</tr>
<tr>
<td>20</td>
<td>funkSbrRatesProxyAcctRequestCurrentRate</td>
<td>ProxyAcctRequest Current Rate</td>
</tr>
<tr>
<td>21</td>
<td>funkSbrRatesProxyAcctRequestAverageRate</td>
<td>ProxyAcctRequest Average Rate</td>
</tr>
</tbody>
</table>
### Table 142: Server Rate Statistics (continued)

<table>
<thead>
<tr>
<th>OID Suffix</th>
<th>Statistic</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>funkSbrRatesProxyAcctRequestPeakRate</td>
<td>ProxyAcctRequest Peak Rate</td>
</tr>
<tr>
<td>23</td>
<td>funkSbrRatesProxyFailTimeoutCurrentRate</td>
<td>ProxyFailTimeout Current Rate</td>
</tr>
<tr>
<td>24</td>
<td>funkSbrRatesProxyFailTimeoutAverageRate</td>
<td>ProxyFailTimeout Average Rate</td>
</tr>
<tr>
<td>25</td>
<td>funkSbrRatesProxyFailTimeoutPeakRate</td>
<td>ProxyFailTimeout Peak Rate</td>
</tr>
<tr>
<td>26</td>
<td>funkSbrRatesProxyFailBadrespCurrentRate</td>
<td>ProxyFailBadresp Current Rate</td>
</tr>
<tr>
<td>27</td>
<td>funkSbrRatesProxyFailBadrespAverageRate</td>
<td>ProxyFailBadresp Average Rate</td>
</tr>
<tr>
<td>28</td>
<td>funkSbrRatesProxyFailBadrespPeakRate</td>
<td>ProxyFailBadresp Peak Rate</td>
</tr>
<tr>
<td>29</td>
<td>funkSbrRatesProxyFailBadsecretCurrentRate</td>
<td>ProxyFailBadsecret Current Rate</td>
</tr>
<tr>
<td>30</td>
<td>funkSbrRatesProxyFailBadsecretAverageRate</td>
<td>ProxyFailBadsecret Average Rate</td>
</tr>
<tr>
<td>31</td>
<td>funkSbrRatesProxyFailBadsecretPeakRate</td>
<td>ProxyFailBadsecret Peak Rate</td>
</tr>
<tr>
<td>32</td>
<td>funkSbrRatesProxyFailMissingresrCurrentRate</td>
<td>ProxyFailMissingresr Current Rate</td>
</tr>
<tr>
<td>33</td>
<td>funkSbrRatesProxyFailMissingresrAverageRate</td>
<td>ProxyFailMissingresr Average Rate</td>
</tr>
<tr>
<td>34</td>
<td>funkSbrRatesProxyFailMissingresrPeakRate</td>
<td>ProxyFailMissingresr Peak Rate</td>
</tr>
<tr>
<td>35</td>
<td>funkSbrRatesProxyRetriesCurrentRate</td>
<td>ProxyRetries Current Rate</td>
</tr>
<tr>
<td>36</td>
<td>funkSbrRatesProxyRetriesAverageRate</td>
<td>ProxyRetries Average Rate</td>
</tr>
<tr>
<td>37</td>
<td>funkSbrRatesProxyRetriesPeakRate</td>
<td>ProxyRetries Peak Rate</td>
</tr>
<tr>
<td>38</td>
<td>funkSbrRatesProxyAuthRejProxyCurrentRate</td>
<td>ProxyAuthRejProxy Current Rate</td>
</tr>
<tr>
<td>39</td>
<td>funkSbrRatesProxyAuthRejProxyAverageRate</td>
<td>ProxyAuthRejProxy Average Rate</td>
</tr>
<tr>
<td>40</td>
<td>funkSbrRatesProxyAuthRejProxyPeakRate</td>
<td>ProxyAuthRejProxy Peak Rate</td>
</tr>
<tr>
<td>41</td>
<td>funkSbrRatesProxyAcctFailProxCurrentRate</td>
<td>ProxyAcctFailProx Current Rate</td>
</tr>
<tr>
<td>42</td>
<td>funkSbrRatesProxyAcctFailProxAverageRate</td>
<td>ProxyAcctFailProx Average Rate</td>
</tr>
<tr>
<td>43</td>
<td>funkSbrRatesProxyAcctFailProxPeakRate</td>
<td>ProxyAcctFailProx Peak Rate</td>
</tr>
<tr>
<td>44</td>
<td>funkSbrRatesProxyAuthRejProxyErrorCurrentRate</td>
<td>ProxyAuthRejProxyError Current Rate</td>
</tr>
<tr>
<td>45</td>
<td>funkSbrRatesProxyAuthRejProxyErrorAverageRate</td>
<td>ProxyAuthRejProxyError Average Rate</td>
</tr>
<tr>
<td>46</td>
<td>funkSbrRatesProxyAuthRejProxyErrorPeakRate</td>
<td>ProxyAuthRejProxyError Peak Rate</td>
</tr>
</tbody>
</table>
Appendix D

Windows Events

Steel-Belted Radius generates a variety of Windows events. Regardless of severity, each event is attributed to one of the following three Windows services: the “core” Steel-Belted Radius service, the authentication service, or the accounting service.

Table 143 lists service identifiers.

<table>
<thead>
<tr>
<th>ID</th>
<th>Symbolic Name</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RADCAT_CORE</td>
<td>Core</td>
</tr>
<tr>
<td>2</td>
<td>RADCAT_AUTH</td>
<td>Authentication</td>
</tr>
<tr>
<td>3</td>
<td>RADCAT_ACCT</td>
<td>Accounting</td>
</tr>
</tbody>
</table>
Table 144 lists events generated for informational purposes only. Informational events do not require operator intervention.

**NOTE:** Some informational events indicate that a previous warning event has been cleared.

### Table 144: Informational Events

<table>
<thead>
<tr>
<th>ID</th>
<th>Informational Event</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>The Steel-Belted Radius service has started.</td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>The Steel-Belted Radius service has stopped.</td>
<td></td>
</tr>
<tr>
<td>102</td>
<td>Count of available threads has risen to acceptable threshold of ( nnnn ).</td>
<td>You can set the threshold value for ( nnnn ) in the [Thresholds] section of the events.ini file.</td>
</tr>
<tr>
<td>103</td>
<td>Amount of free file system space has risen to acceptable threshold. Free byte count is ( nnnnnnnn ).</td>
<td>You can set the threshold value for ( nnnnnnnn ) in the [Thresholds] section of the events.ini file.</td>
</tr>
<tr>
<td>104</td>
<td>Steel-Belted Radius has reconnected to the Service Level Manager server after a ConcurrencyFailure.</td>
<td></td>
</tr>
<tr>
<td>105</td>
<td>Steel-Belted Radius has reconnected to the SQL database after a SQLConnectFail.</td>
<td></td>
</tr>
<tr>
<td>106</td>
<td>Steel-Belted Radius has reconnected to the LDAP database after an LDAPConnectFail.</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>A user’s account has been locked due to excessive authentication attempts within a specified period.</td>
<td></td>
</tr>
<tr>
<td>108</td>
<td>A user account, previously locked due to an excessive amount of rejected authentication attempts, has been unlocked.</td>
<td></td>
</tr>
<tr>
<td>109</td>
<td>The target server for proxy spooling has reconnected.</td>
<td></td>
</tr>
</tbody>
</table>
Warning Events

Table 145 lists warning events, that may require operator intervention.

Some warning events can be diluted, meaning that a warning message is generated every nnnn times an event occurs. Warning message dilution is configured in the [EventDilutions] section of the events.ini file.

<table>
<thead>
<tr>
<th>ID</th>
<th>Warning Event</th>
<th>Dilutable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>5001</td>
<td>Count of available threads has dropped to the minimum threshold of nnnn.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Indicates that a low thread count available condition has been detected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This event can be issued in the authentication or accounting category to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicate a shortage of authentication or accounting threads.</td>
<td></td>
</tr>
<tr>
<td>5002</td>
<td>Concurrency server returned failure indication. This event represents nnnn</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>failures.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates that a reject was returned from the Service Level Manager server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(concurrency server) in response to a proxied authentication request.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The reject was for a reason other than exceeded port limit.</td>
<td></td>
</tr>
<tr>
<td>5003</td>
<td>Timed out in proxy attempt to concurrency server. This event represents</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>nnnn requests timing out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates that a time-out was encountered when proxy-forwarding an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>authentication request to the Service Level Manager server (concurrency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server).</td>
<td></td>
</tr>
<tr>
<td>5004</td>
<td>Local failure encountered in attempt to proxy to concurrency server. This</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>event represents nnnn requests timing out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates that a local processing failure was encountered when trying to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>proxy-forward an authentication request to the Service Level Manager server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(concurrency server).</td>
<td></td>
</tr>
<tr>
<td>5005</td>
<td>Timed out in static accounting proxy attempts. This event represents nnnn</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>failures.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates that a time-out was encountered when proxy-forwarding an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>accounting request to the Service Level Manager server (concurrency server).</td>
<td></td>
</tr>
<tr>
<td>5006</td>
<td>Local failure encountered in attempt to proxy for static accounting. This</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>event represents nnnn requests timing out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates that a local processing failure was encountered when trying to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>proxy-forward an accounting request to the Service Level Manager server (</td>
<td></td>
</tr>
<tr>
<td></td>
<td>concurrency server).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can set the threshold value for nnnnn using the [EventDilutions]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>section of events.ini.</td>
<td></td>
</tr>
<tr>
<td>5007</td>
<td>Amount of free file system space has dropped below minimum threshold.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Free byte count is nnnnnnnnnn.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can set the threshold value for nnnnnnnnn in the [Thresholds] section</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of events.ini.</td>
<td></td>
</tr>
<tr>
<td>5008</td>
<td>nnnn attempts to connect to SQL server failed.</td>
<td>Yes</td>
</tr>
<tr>
<td>5009</td>
<td>nnnn disconnects from SQL server due to error.</td>
<td>Yes</td>
</tr>
<tr>
<td>5010</td>
<td>nnnn timeouts on SQL requests.</td>
<td>Yes</td>
</tr>
<tr>
<td>5011</td>
<td>Access to accounting server database has timed out. This event represents</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>nnnn timeouts.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 145: Warning Events (continued)

<table>
<thead>
<tr>
<th>ID</th>
<th>Warning Event</th>
<th>Dilutable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>5012</td>
<td>Access to accounting server database has failed. This event represents <code>nnnn</code> failures.</td>
<td>Yes</td>
</tr>
<tr>
<td>5013</td>
<td>Verification Server has timed out. This event represents <code>nnnn</code> Verification Server timeouts.</td>
<td>Yes</td>
</tr>
<tr>
<td>5014</td>
<td>Verification Server requests have failed. This event represents <code>nnnn</code> Verification Server failures.</td>
<td>Yes</td>
</tr>
<tr>
<td>5015</td>
<td>The connection to an LDAP server has failed.</td>
<td>No</td>
</tr>
<tr>
<td>5016</td>
<td>Communication with an LDAP server has failed. This event represents <code>nnnn</code> connection failures.</td>
<td>Yes</td>
</tr>
<tr>
<td>5017</td>
<td>The LDAP server has disconnected. This event represents <code>nnnn</code> connection failures.</td>
<td>Yes</td>
</tr>
<tr>
<td>5018</td>
<td>A request to the LDAP server has timed out. This event represents <code>nnnn</code> request timeouts.</td>
<td>Yes</td>
</tr>
<tr>
<td>5019</td>
<td>The LDAP server has disconnected</td>
<td>No</td>
</tr>
<tr>
<td>5020</td>
<td>A request to the LDAP server has timed out.</td>
<td>No</td>
</tr>
<tr>
<td>5021</td>
<td>The target server of proxy spooling fails to respond (non-dilutable).</td>
<td>No</td>
</tr>
<tr>
<td>5022</td>
<td>The target server of proxy spooling fails to respond (dilutable).</td>
<td>Yes</td>
</tr>
<tr>
<td>5023</td>
<td>A port allocation hard limit has been reached for realm <code>xxxx</code>. This represents a total of <code>nnnn</code> hard limit violations for all servers.</td>
<td>Yes</td>
</tr>
<tr>
<td>5026</td>
<td>A port allocation hard limit has been reached for realm <code>xxxx</code>. This represents a total of <code>nnnn</code> hard limit violations for all servers.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Error Events

Error events usually require some form of operator intervention.

Most Steel-Belted Radius error events are generated at startup, as the service initializes its components. If a component fails at startup, the start operation is aborted and the system generates an error event. The text of the error event message identifies what Steel-Belted Radius was doing when it failed. In some cases, the operator can take direct action in response to an error event. For example, if the system is unable to open a log file, the system disk might be full, leaving no room to create additional files.

The event text identifies the problem area in the software. You should escalate the problem to your next level of support. When you do, be sure to indicate the ID, name, and text of the event.

Table 146: Error Events

<table>
<thead>
<tr>
<th>ID</th>
<th>Error Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td>StartServiceCtrlDispatcher failed with error nnnn.</td>
</tr>
<tr>
<td>10001</td>
<td>SetServiceStatus failed with error nnnn.</td>
</tr>
<tr>
<td>10002</td>
<td>Invalid private directory 'directory' specified.</td>
</tr>
<tr>
<td>10003</td>
<td>Unable to create thread.</td>
</tr>
<tr>
<td>10004</td>
<td>Unable to create mutex.</td>
</tr>
<tr>
<td>10005</td>
<td>Unable to initialize signal handling</td>
</tr>
<tr>
<td>10006</td>
<td>Unable to configure event processing</td>
</tr>
<tr>
<td>10007</td>
<td>Unable to create or open log file</td>
</tr>
<tr>
<td>10008</td>
<td>Unable to initialize LDAP administration interface.</td>
</tr>
<tr>
<td>10009</td>
<td>Unable to initialize RPC administration interface.</td>
</tr>
<tr>
<td>10010</td>
<td>Unable to initialize base IP interface.</td>
</tr>
<tr>
<td>10011</td>
<td>Unable to initialize current user list processing.</td>
</tr>
<tr>
<td>10012</td>
<td>Unable to initialize challenge continuation cache.</td>
</tr>
<tr>
<td>10013</td>
<td>Unable to initialize network access device activity monitor.</td>
</tr>
<tr>
<td>10014</td>
<td>Unable to initialize dictionary processing.</td>
</tr>
<tr>
<td>10015</td>
<td>Unable to process vendor.ini file</td>
</tr>
<tr>
<td>10016</td>
<td>Unable to initialize Btrieve</td>
</tr>
<tr>
<td>10018</td>
<td>Unable to initialize admin user rights component.</td>
</tr>
<tr>
<td>10019</td>
<td>Unable to open Btrieve</td>
</tr>
<tr>
<td>10020</td>
<td>Unable to initialize tunnel DNIS lookup component.</td>
</tr>
<tr>
<td>10021</td>
<td>Unable to initialize configuration caching component.</td>
</tr>
<tr>
<td>10022</td>
<td>Unable to initialize database caching component.</td>
</tr>
<tr>
<td>10023</td>
<td>Unable to initialize license processing</td>
</tr>
<tr>
<td>10024</td>
<td>Unable to initialize NDS trustee processing.</td>
</tr>
</tbody>
</table>
**Table 146: Error Events (continued)**

<table>
<thead>
<tr>
<th>ID</th>
<th>Error Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>10025</td>
<td>Unable to initialize NetWare host lookup processing.</td>
</tr>
<tr>
<td>10026</td>
<td>Unable to initialize IP/IPX pool resource management.</td>
</tr>
<tr>
<td>10027</td>
<td>Unable to initialize user login count tracking.</td>
</tr>
<tr>
<td>10028</td>
<td>Unable to create persistent store for Sessions list.</td>
</tr>
<tr>
<td>10029</td>
<td>Unable to initialize persistent store for Sessions list.</td>
</tr>
<tr>
<td>10030</td>
<td>Unable to initialize performance monitor interface component.</td>
</tr>
<tr>
<td>10031</td>
<td>Unable to initialize admin locking component.</td>
</tr>
<tr>
<td>10032</td>
<td>Unable to initialize plug-in support component.</td>
</tr>
<tr>
<td>10033</td>
<td>Unable to initialize duplicate request cache.</td>
</tr>
<tr>
<td>10034</td>
<td>Unable to initialize name mangling support.</td>
</tr>
<tr>
<td>10035</td>
<td>Unable to initialize name stripping support.</td>
</tr>
<tr>
<td>10036</td>
<td>Error nnnn returned from call to GetDiskFreeSpaceEx. File system space checking disabled.</td>
</tr>
<tr>
<td>10037</td>
<td>Unable to initialize name validation support. Service start aborted.</td>
</tr>
<tr>
<td>10038</td>
<td>Unable to initialize system resource checking. Service start aborted.</td>
</tr>
<tr>
<td>10039</td>
<td>Unable to initialize statistic collection. Service start aborted.</td>
</tr>
<tr>
<td>10040</td>
<td>Attempt to connect to SQL server xxxxxxxxxx failed.</td>
</tr>
<tr>
<td>10041</td>
<td>Disconnect from SQL server xxxxxxxxxx due to error.</td>
</tr>
<tr>
<td>10042</td>
<td>Timeout on SQL request.</td>
</tr>
<tr>
<td>10043</td>
<td>Unable to allocate reserved memory specified by ReserveMemoryKB. You can set the ReserveMemoryKB value in the [Thresholds] section of the events.ini configuration file.</td>
</tr>
<tr>
<td>10044</td>
<td>Memory allocation failure encountered. Reserved memory released as last resort.</td>
</tr>
<tr>
<td>10045</td>
<td>nnnn memory allocation failures have occurred. You can set the threshold value for nnnn using the [EventDilutions] section of events.ini.</td>
</tr>
<tr>
<td>10046</td>
<td>The connection to the Accounting Server has failed.</td>
</tr>
<tr>
<td>10047</td>
<td>The connection to the Verification Server has failed.</td>
</tr>
<tr>
<td>10050</td>
<td>The initialization of common IP services at server startup has failed.</td>
</tr>
</tbody>
</table>
Symbols

%Alias .................................................. 235, 256
%AllowedAccessHours ......................... 260
%DN .................................................. 257
%EffectiveRealm ................................. 260
%EffectiveUser .................................. 260
%FullName ........................................ 235, 256
%LoginLimit ...................................... 234, 255
%Name ............................................... 259
%NASAddress .................................... 260
%NASModel ........................................ 260
%NASName .......................................... 260
%OriginalUserName ............................. 259
%Password ......................................... 234, 255, 260
%ProxyRealm ..................................... 235, 255
%ProxyUserName ................................. 235, 255
%RADIUSClientName ............................ 260
%Realm ............................................ 260
%User ............................................... 259
%UserName ........................................ 259
* .pro ............................................. 149, 232
.aut .................................................. 232

A
Accept .............................................. 30, 233, 269
AcceptReport section .......................... 73
Access .............................................. 11
access.ini .......................................... 2
Groups ............................................ 8
Users ............................................... 8
AccessLevel ..................................... 10
account.ini ........................................ 2
Alias/name ....................................... 142
Attributes ....................................... 143
Configuration .................................. 144
Settings .......................................... 144
TypeNames ...................................... 147
Acct section
 in *.dir files .................................... 178
 in *.pro files .................................. 122
AcctAttributeMap section
 in proxy.ini .................................... 157
AcctAutoStopEnable ............................ 26
AcctMethods section

Index
<table>
<thead>
<tr>
<th>Discard-After</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard-Before</td>
<td>128</td>
</tr>
<tr>
<td>Driver</td>
<td>239, 245</td>
</tr>
</tbody>
</table>

### E

**eap.ini** ...............................................................3, 184, 213, 222
**EAP-15** ...............................................................93
**EAP-32** ...............................................................93
**EAP-Only** .............................................................185
**EAP-Type** .............................................................185

**EmbedInClass section**

- in radius.ini ...............................................................56
- Enable15, 70, 73, 74, 88, 89, 134, 145, 164, 166, 174, 177, 179, 187, 193, 215, 252, 244, 253
- EnableEricssonViGHTTPDigestSupport ..............................................................29
- EnableHTTPDigestSupport ..............................................................29
- encryption key ..................................................................................4, 126
- EnhancedDiagnosticLogging .....................................................................30
- EOTP .................................................................................................93
- Ericsson ViG .......................................................................................29
- eval.ini ..............................................................................................18

**EventDilutions section**

- in events.ini .....................................................................................19
- events.ini .............................................................................................3, 19
- EXCLUDE ..............................................................................................119
- exponentiation .....................................................................................188, 194, 200, 207, 216
- Extended One-Time Password ..................................................................93
- ExtendedProxy ........................................................................................30, 181

### FailedAuthOriginStats section

- in radius.ini ..........................................................................................37

**Failure section**

- aut file .........................................................................................268
- in *.aut ..........................................................................................235
- fastauth.aut .....................................................................................3, 187

**FastFail section**

- in *.pro files .....................................................................................172

**file permissions** ..................................................................................51

**FileSystemFreeKBWarningClear** ..........................................................20
**FileSystemFreeKBWarningIssue** ..........................................................20

**Filter** ...............................................................................................258

**filter rules** ..........................................................................................119

**filter.ini** ..............................................................................................3, 149, 152

**FilterIn** ..............................................................................................165, 167
**FilterOut** ..............................................................................................164, 167

**first column, configuration files** ...................................................................6
**First-Handle-Via-Auto-EAP** .....................................................................185

**FlashReconnect** ..................................................................................263, 266
**FramedIPAddressHint** ............................................................................30

**FullName** ............................................................................................233, 269

**Funk-Allowed-Access-Hours attribute** ..................................................273
**Funk-Concurrent-Login-Limit attribute** ..................................................273
**Funk-Full-User-Name attribute** ...............................................................273

**Funk-Full-User-Name attribute** ..................................................................273

**Funk-Location-Group-Id attribute** .........................................................27, 273
**Funk-Peer-Cert-Hash attribute** ..................................................................273
**Funk-Peer-Cert-Issuer attribute** ..................................................................273
**Funk-Peer-Cert-Principal attribute** ..........................................................274
**Funk-Peer-Cert-Subject attribute** ............................................................274
**Funk-Radius-Client-Group attribute** .......................................................27
**Funk-Round-Robin-Group attribute** ..........................................................274
**Funk-Source-IP-Address attribute** ..........................................................274
**Funk-Source-IPV6-Address attribute** .......................................................274
**Funk-Tribe-Name attribute** .................................................................274

### G

**gedit** .................................................................................................5

### H

**hex4** .................................................................................................113
**hexadecimal** .......................................................................................113

### I

**Ignore-Acct-SS** ....................................................................................129
**ignore-ports** ......................................................................................129
**ImportExport** ......................................................................................12
**in authlog.ini** .....................................................................................68
**in authReport.ini** ..................................................................................73
**IncludeProxy** ........................................................................................88

**InitializationString** ...............................................................................106, 187, 193, 215, 232, 253
**int** ...................................................................................................113
**int4** ...................................................................................................113
**integer** ................................................................................................113

**Interval-Seconds** .....................................................................................99
**IP address pool** .....................................................................................35
**ipaddr** .................................................................................................113
**ipaddr-pool** ...........................................................................................113
**IP-Pools** ..............................................................................................12
**IPPoolSuffixes section**

- in radius.ini ..........................................................................................38

**IPv6 section**

- in radius.ini ..........................................................................................39
**ipxaddr-pool** ..........................................................................................113
**IPX-Pools** ............................................................................................12

### Index
J
JDBC ................................................. 232

K
Keys section
in spi.ini ........................................ 126

L
LastResort ........................................ 263
LDAP section
in radius.ini ................................ 39
LDAPAddresses section
in radius.ini .................................. 40
ldapauth.aut ................................... 3, 252
LdapVersion .................................. 263, 266
LeaseTime .................................... 136
LibraryName ................................. 187, 193, 215, 232, 244, 253
License ........................................ 12
LineSize .................................. 71, 76, 79, 83, 86, 145
load balancing ............................. 249
LocalPort .................................. 155
Lockout ..................................... 89
lockout.ini ................................... 3, 89
log file
  size limit .................................. 31
LogAccept ................................... 30
LogDir ........................................ 30
LogFileMaxMBytes ......................... 31
LogFilePermissions ........................ 31, 71, 76, 79, 83, 86, 99, 145
LogHighResolutionTime ................. 31
LogLevel ................................... 31, 240, 245, 266
LogReject ................................... 32

M
machine authentication .................. 107, 185
macro records .............................. 115
MaxConcurrent ............................ 240, 245, 247, 263, 267
Max-EAP-Fragment ......................... 129
MaxMinutePerFile ......................... 76, 80, 83, 86
MaxPong ..................................... 16
MaxScriptSteps ................................ 267
MaxShutdown ................................ 16
MaxSize ................................... 71, 145
MaxStartup .................................. 16
MaxWaitReconnect ......................... 240, 245, 263, 267
MessageAuthenticator .................... 165
MinFailures ................................ 173
MinLeaseTime ................................ 136
MinSeconds ................................ 173
ModifyUser section
  in *.dir .................................. 180
  in * pro .................................. 173
MS-CHAP
  name stripping .......................... 40
  MsChapNameStripping .................. 40

N
name stripping, MS-CHAP ................ 40
Native User authentication ............. 214
negative number in attribute .......... 113
New PIN mode ............................ 92
NoNullTermination ....................... 32
Notepad .................................... 5
null terminator ........................... 113
NumAttempts ................................ 165, 167

O
OnFound ................................ 257, 267
OnNotFound ................................ 257, 267
Oracle .................................... 232, 244
OverallTimeout ........................... 134

P
Pad ............................................ 135
ParameterMarker ......................... 240, 245
Password .................................. 263, 267
PasswordCase ............................. 267
PasswordFormat ......................... 240, 267
PEAP_Max_Version ....................... 195
PEAP_Min_Version ....................... 194
peapauth.aut ................................ 3, 122, 193
permissions ................................ 51
PhantomTimeout ........................... 32
PIN ........................................... 92
PIN, system-generated ................. 92
PingInterval ................................
  pool.dhc .................................. 136
  Request section ....................... 136
  Settings section ...................... 136
PoolPctAddressAvailWarningClear .... 21
PoolPctAddressAvailWarningIssue ... 20
Pools section
  dhcp.ini .................................. 135
  Port ....................................... 263
  port number, SNMP ..................... 228
  port-number-usage .................... 129
Ports section
  in radius.ini ............................ 42
  POTP ...................................... 93
PrequalifyChecklist ...................... 108
PrivateDir .................................. 32
Processing section
  in proxy.ini ............................ 157
ProcessRealmBeforeTunnel ............. 32
Product-Scan-Acct ....................... 130
product-scan-acct ....................... 129
Product-Scan-Auth ....................... 130
product-scan-auth ....................... 129
<table>
<thead>
<tr>
<th><strong>Profile</strong></th>
<th>88, 233, 269</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProfileForExpiredUsers</td>
<td>107</td>
</tr>
<tr>
<td>ProfileForExpiredUsersInGroups</td>
<td>107</td>
</tr>
<tr>
<td>Profiles</td>
<td>12</td>
</tr>
<tr>
<td>Protected One-Time Password</td>
<td>93</td>
</tr>
<tr>
<td>Proxy</td>
<td>12</td>
</tr>
<tr>
<td>proxy accounting</td>
<td>160</td>
</tr>
<tr>
<td>proxy.ini</td>
<td>3, 150, 155</td>
</tr>
<tr>
<td>ProxyFastFail</td>
<td>32, 172</td>
</tr>
<tr>
<td>proxyrl.ini</td>
<td>3</td>
</tr>
<tr>
<td>ProxySource</td>
<td>33</td>
</tr>
<tr>
<td>ProxyStripRealm</td>
<td>33</td>
</tr>
</tbody>
</table>

**Q**

| Quarantine_Profiles         | 221         |
| QueryTimeout                | 240, 244, 246, 247, 263 |
| QuoteBinary                 | 71, 77, 80, 83, 87, 145 |
| QuotefromTime                | 71, 77, 80, 83, 87, 145 |
| QuoteIPAddress              | 72, 77, 80, 83, 87, 146 |
| QuoteText                   | 72, 77, 80, 83, 87, 146 |
| QuoteTime                   | 72, 77, 80, 84, 87, 146 |

**R**

| RADIUS                      | 52          |
| radius.ini                  | 3, 22, 53, 60, 150, 153, 154 |
| AuthRejectLog               | 24          |
| Configuration               | 26          |
| CurrentSessions             | 35          |
| EmbedInClass                | 36          |
| FailAuthOriginStats         | 37          |
| HiddenEAPIdentity           | 37          |
| IPPoolSuffixes              | 38          |
| IPv6                        | 39          |
| LDAP                        | 39          |
| LDAPAddresses               | 40          |
| Ports                       | 42          |
| SecurID                     | 44          |
| Self                        | 44          |
| StaticAcctProxy             | 45          |
| Strip                       | 45          |
| ValidateAcct                | 48          |
| ValidateAuth                | 48          |
| RADIUS_HIGH_FDS             | 52          |
| RADIUS_PRIVATE_DIR          | 52          |
| radiusdir                   | xii         |
| RADIUSARGS                  | 52          |
| radsql_acct_jdbc.so         | 244         |
| radsql_auth_jdbc.so         | 232         |
| RAS-Clients                 | 12          |
| Realms section              |             |
| in proxy.ini                | 156         |
| RecordLocally               |             |
| redirect.ini                |             |
| RegularExpression           | 49          |
| Reject                      | 32          |
| RejectReport section        |             |
| in authReport.ini           | 74          |
| Rejects                     | 32          |
| REPLACE                     | 119         |
| Report                      | 13          |
| Request section             |             |
| in *.aut                    | 259         |
| RequestTimeout              | 165, 167    |
| RequestTimeoutMills         | 165, 167    |
| Require_Client_Certificate  | 216         |
| ReserveMemoryKB             | 20          |
| ResetSeconds                | 173         |
| ResetStats                  | 59          |
| ResetThreadHighWaterMarks   | 59          |
| Response section            |             |
| in *_.aut                   | 254         |
| Results section             |             |
| Search                      | 257, 263, 268 |
| Search/name section         |             |
| in *.aut                    | 256         |
| SecondsToCachePasscodes     | 44          |
| section headers             | 5           |
| SecureTcpAdminPort          | 42          |
| SecurID section             |             |
| in radius.ini               | 44          |
| securid.ini                 | 4, 92       |
| securidauth.aut             | 4           |
| SelectIPPoolNameByNasAVPs   | 33          |
| Self section                |             |
| in radius.ini               | 44          |
| Send-Class-Attribute        | 129         |
| SendOnlyOneClassAttribute   | 34          |
| send-session-timeout-on-challenge | 129 |
| server log file             |             |
| size limit                  | 31          |
| Server section              |             |
| in *.aut                    | 264         |
in *.aut .......................................................... 236
Server/name section
aut file ............................................................ 237, 261
ServerInfo section
in tacplus.ini .................................................. 105
ServerPort ....................................................... 135
servtype.ini ................................................... 4, 55
Settings section
aut file ............................................................ 265
in *.aut .......................................................... 238
in account.ini .................................................. 144
in authlog.ini .................................................... 70
in authReportAccept.ini ................................... 75
in authReportBadSharedSecret.ini ................. 79
in authReportReject.ini ................................... 82
in authReportUnknownClient.ini .................... 86
in bounce.ini ................................................... 15
in dhcp.ini ...................................................... 134
in lockout.ini ................................................... 89
in pool.dhc files ............................................ 136
SharedSecret .................................................. 105
ShutdownDelay ............................................... 174
sidalt.aut ....................................................... 4
signed integer, as attribute type .................... 113
signed-integer ............................................... 113
Simple Network Management Protocol, see SNMP
size limit in server log ..................................... 31
smart static accounting .................................... 163
SNMP .......................................................... 223
port ............................................................... 228
subagent ........................................................ 229
system contact ............................................... 226
spi.ini ............................................................ 4, 126
SpooledAccounting section
in *.pro ......................................................... 174
SQL ............................................................. 240, 247
sqlacct.acc .................................................... 5, 4, 244
sqlauth.aut .................................................... 5, 4, 232
SSL ............................................................... 263
StartupTimeout ................................................ 34
static proxy accounting ................................... 160
StaticAcct section
in proxy.ini .................................................. 160
StaticAcctProxy section
in radius.ini .................................................. 45
StaticAcctRealms .......................................... 167, 179
Statistics ....................................................... 13
statlog.ini ..................................................... 98
string .......................................................... 115
stringnz ........................................................ 113
Strip section
in *.aut .......................................................... 241
in radius.ini .................................................. 45
StripRealm ..................................................... 165, 168, 177, 179
subagent, SNMP ............................................. 229
SuccessResult ................................................ 240
Suppress section
in events.ini ................................................... 19
syscontact ...................................................... 226
syslocation ..................................................... 226
sysname ......................................................... 226
system contact ............................................... 226
system-generated PIN ..................................... 92
T
TACACS+ ...................................................... 105
tacplus.ini ...................................................... 4, 105
TargetAddress ............................................... 136
TargetHost ..................................................... 105
TargetsSection ............................................. 164, 166, 168
TCPControlAddress ....................................... 43
TCPControlPort ........................................... 43
testagent.sh .................................................... 230
ThreadAvailWarningClear ................................ 20
ThreadAvailWarningIssue ............................... 20
Thresholds section
in events.ini ................................................... 20
time .............................................................. 113
time attribute ............................................... 113
Timeout ......................................................... 268
Titles .............................................................. 72, 146
tlsauth.aut ..................................................... 4
tlsauth.eap ..................................................... 4
TraceLevel .................................................... 34
transforming user names ................................. 46
trap2sink ....................................................... 227
trapcommunity ............................................. 227
trapsink ......................................................... 227
TreatAddressPoolsAsDisjoint ......................... 35
tlsauth.aut ..................................................... 4, 122, 215
Tunnels ........................................................... 13
Type section
acc file .......................................................... 246
Type/statement section
acc file .......................................................... 247
TypeNames section
acc file .......................................................... 248
in account.ini ............................................... 147
U
UDPAcctPort .................................................. 43
UDPAuthPort .................................................. 43
UDPProxyPortBlockLength .............................. 43
UDPProxyPortBlockStart ............................... 43
ULIMIT_CORE_COUNT .................................... 51
ULIMIT_CORE_SIZE ....................................... 51
ULIMIT_OPEN_FILES ...................................... 51
umask ........................................................... 51
Index

uniport.aut .............................................................. 5
UnknownClientReport section
  in authReport.ini .................................................. 74
unsigned integer, as attribute type ................. 113
update.ini ............................................................... 5, 58
Update3GPP2 .......................................................... 59
UpdateAdminAccess ................................................. 59
UpdateAutoStop ...................................................... 59
UpdateCCAGateways .............................................. 60
UpdateDHCPPools .................................................. 60
UpdateEAP .............................................................. 60
UpdateLogAndTraceLevel ....................................... 60
UpdateLogfilePermissions ...................................... 60
UpperCaseName ..................................................... 240, 246, 268
UseMasterDictionary .............................................. 166, 168
UseNewAttributeMerge ......................................... 35
user names
  transforming ...................................................... 46
User-Name ............................................................. 48
Users ................................................................. 13
Users section
  in access.ini ....................................................... 8
USR2 signal .......................................................... 58
UTC ........................................................................ 72, 77, 80, 84, 87, 146, 246, 268

V
ValidateAcct section
  in radius.ini .......................................................... 48
ValidateAuth section
  in radius.ini .......................................................... 48
vendor.ini ............................................................. 5, 128
Vendor-Product ...................................................... 130
ViG ................................................................. 29

W
WaitReconnect ..................................................... 241, 246, 263
WATCHDOG ........................................................... 52
WATCHDOGARGS ................................................... 52
WATCHDOGENABLE ............................................... 52
WATCHDOGOPTS .................................................. 52
winauth.aut ........................................................... 5, 106
WindowsDomain section .................................... 106
Within ............................................................... 89

Y
yyyyymmdd.log ..................................................... 31